СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(5.07–18.07)

2018 № 14

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(5.07–18.07)
№ 14

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

9.07.2018
WhatsApp получил поддержку самой долгожданной функции

Разработчики WhatsApp выпустили обновленную версию мессенджера, в которой появилась поддержка специальной функции, позволяющей преобразовать групповой чат в канал.

Докладніше

***

12.07.2018
В Instagram появились интерактивные стикеры-вопросы. Как ими пользоваться?

В приложениях Instagram для iOS и Android появилась новая функция – интерактивные стикеры-вопросы для «Историй». С помощью них любой пользователь может спросить о чем-нибудь автора сториз или ответить на интересующие подписчиков вопросы. Все вопросы и их отправители видны только опубликовавшему историю пользователю (InternetUA).

При ответе на каждый из вопросов автоматически создается новый пост в «Историях», при этом текст сообщения виден всем, а имя отправителя скрыто. Все вопросы собираются в отдельный список, который находится в одном меню со статистикой сториз. Стиль наклейки можно редактировать – изменять оформление, цвет, размер и угол наклона.

Чтобы воспользоваться новой функцией, нужно прикрепить к истории соответствующий стикер, настроить его по вашему вкусу и опубликовать пост. Количество вопросов, которые можно задать под одной сториз, не ограничено.

Руководство сервиса считает, что новые стикеры помогут блогерам и популярным пользователям более тесно взаимодействовать со своей аудиторией. Так, например, можно один раз ответить на популярный вопрос, который постоянно задают в комментариях или Direct, и ответ на него увидят все подписчики.

***

17.07.2018
В Skype появится долгожданная возможность

Microsoft сообщила, что Skype наконец-таки получит долгожданную миллионами пользователей возможность записывать звонки. Функция, уже давно присутствующая в бизнес-версии Skype, наконец добралась до обычной потребительской версии сервиса спустя 15 лет с момента запуска. Запись

звонков будет происходить в облаке, так что пользователи смогут получить доступ к видеозаписям из любого устройства (вопрос приватности), будь то Windows, Mac, iOS, Android или даже Linux. Как только один из участников диалога начнет записывать беседу, другие получат уведомление, что надо бы прикусить язык и не взболтнуть лишнего. Skype будет записывать видеопоток каждого собеседника, а также трансляцию экранов. Благодаря этому нововведению пользователям больше не надо будет использовать сторонние приложения для записи диалогов. Достаточно будет начать чат, нажать на соответствующую кнопку и дело в шляпе (InternetUA).

Рассылка новой функции записи звонков начнется в конце текущего месяца. Все пользователи получат к ней доступ в недалеком будущем. Приятно видеть, что кроме редизайнов и никчемных историй, разработчики помнят о необходимости внедрять в сервис действительно полезные и востребованные возможности. И плевать, что на их реализацию понадобилось всего лишь 15 лет.

***

16.07.2018
Аккаунты в соцсетях будут переходить по наследству

Жители Германии с 2012 года пытались получить доступ к Facebook своей дочери, покончившей с собой в берлинском метро. Соцсеть отказывала им в этом, ссылаясь на защиту конфиденциальных данных, и отстаивала свою позицию в суде (InternetUA).

После нескольких апелляций Федеральный верховный суд Германии всё же обязал Facebook предоставить родителям логин и пароль их дочери, указав, что они имеют на это право, согласно закона о цифровом наследии. В своём решении суд указал, что записи в Facebook можно рассматривать наравне с бумажными письмами и дневниками, которые после смерти человека переходят по наследству к его родным.

Это первый судебный прецедент такого рода в Европе. Скорее всего, теперь суды при рассмотрении аналогичных исков будут ссылаться на это решение и обязывать соцсети предоставлять наследникам доступ к аккаунтам умерших людей. В настоящее время Facebook замораживает страницы покойников, превращая их в цифровые мемориальные доски, но не предоставляет родственникам доступ к личной переписке и записям, скрытым от просмотра.

***

17.07.2018
Ирина Фоменко
У Facebook появится «безопасный» конкурент

Активисты по защите личной информации запускают конкурента

Facebook, стремясь заполучить недовольных пользователей медиа-гиганта после скандала Cambridge Analytica. Об этом сообщает The Telegraph (InternetUA).

Согласно краудфандинговой кампании, веб-сайт Openbook создан для изменения восприятия социальных сетей: от «все ради денег» и «не задумываюсь о последствиях» к тому, что можно будет называть «замечательным». Разработчики сайта хотят «постить забавные видео с кошками», не ставя под угрозу неприкосновенность частной жизни.

Сайт, 30 % прибыли которого будет выделяться на благотворительность, спонсируется Филиппом Циммерманом (создал программное обеспечение для шифрования электронной почты PGP).

Социальную сеть разработал инженер по кибербезопасности Джоэл Эрнандес. По его словам, он хотел основать конкурента Facebook уже давно, и сейчас создает альтернативу после скандала компании с Cambridge Analytica.

Несмотря на скандал, у Facebook 2,2 млрд активных пользователей. Ежедневно в социальной сети регистрируются тысячи человек.

Помимо того, что аудиторская группа контролирует работу разработчиков, Openbook планирует получить выгоду от новых правил по защите данных. Европейский закон позволяет пользователям легко перенести свои данные из Facebook и Twitter на другой сайт.

Кроме того, новая социальная сеть стремится не вызывать привыкание у пользователей, в отличие от Facebook. В планах у Openbook – открыть маркетплейс и сократить количество онлайн-транзакций.

Средства на запуск сайта начнут собрать с 17 июля на Kickstarter. Инвесторы в качестве подарка получат фирменные футболки и кружки, а также доступ к бета-версии социальной сети.

***

17.07.2018

Facebook отправила «бота-туриста» исследовать виртуальный Нью-Йорк

Компания Facebook провела эксперимент, в рамках которого отправила «бота-туриста» исследовать 360-градусные изображения Адской кухни, одного из районов Нью-Йорка. В помощь ему был предоставлен «бот-гид», использовавший двухмерные карты. Первый должен был описывать, где он находится, по тому, что видит, а второй сообщал ему, куда двигаться дальше (InternetUA).

Проект был направлен на сбор информации посредством простого человеческого языка – например, бот мог использовать фразу «передо мной находится магазин Brooks Brothers». Но в ходе эксперимента исследователи выяснили, что боты работают эффективнее, если используют для общения своего рода синтетический язык, состоящий из символов. Другими словами, для того, чтобы помочь человеку найти нужную гостиницу, искусственный

интеллект должен использовать другой язык, нежели для взаимодействия, скажем, с самоуправляемым автомобилем.

Исследование также помогло ИИ разобраться в визуально сложном городском окружении. Специальная система быстро анализировала наиболее подходящие слова в ответах ботов, чтобы они могли точнее сообщать, где находятся и куда должны двигаться дальше.

Этот проект может улучшить ИИ в целом, а не только помочь создать продвинутый навигационный продукт. Например, самоуправляемым автомобилям и заблудившимся людям было бы проще находить дорогу, не имея доступа к GPS.

***

17.07.2018

Аккаунты Facebook и Instagram можно будет синхронизировать

Компания Facebook в данный момент тестирует возможность, которая должна подтолкнуть пользователей Messenger также активнее использовать социальную сеть Instagram (InternetUA).

Речь идет о возможности синхронизировать аккаунты из обеих социальных сетей. Ранее в Facebook Messenger уже появилась возможность добавления своей учетной записи в Instagram, однако пока что возможностей для синхронизации между ними не было.

После того, как вы свяжите учетную запись Instagram с Facebook Messenger, у вас появится возможность использовать свое Instagram-имя в Messenger и находить в мессенджере своих друзей по их никам в Instagram.

Пока что функция тестируется ограниченным количеством пользователей, точная дата выхода обновления для всех пока не сообщается.

***

18.07.2018

WhatsApp получил самую долгожданную функцию этого года

В большинстве мессенджеров давно присутствуют стикеры, причем в некоторых у пользователей есть возможность создавать собственные наборы, используя любые изображения (InternetUA).

Поддержка стикеров, по всей видимости, появится и в WhatsApp. Об этом свидетельствуют данные, полученные сайтом WABetaInfo.

Ресурс отмечает, что в актуальной версии WhatsApp стикеров нет - речь идет о будущих версиях. Стикеры будут доступны в специализированном каталоге-магазине.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

10.07.2018

Українці завалили рейтинг FIFA у Facebook і тисячами залишають коментарі «Слава Україні»

Всього один день знадобився українцям, щоб опустити майже до «1» рейтинг FIFA у Facebook. Станом на ранок 10 липня вже було 150 тисяч «одиниць» залишених переважно українцями (Watcher).

Окрім того, під постами цієї організації українці масово пишуть коментарі зі словами «Слава Україні», «Glory to Ukraine». Якщо раніше середньостатистичний пост FIFA набирав в кращому випадку кілька десятків коментарів, то зараз їх там тисячі.

В такий спосіб українці висловлюють свою зневагу до цієї футбольної організації через попередження гравцю збірної Хорватії Домагою Віді за вислів «Слава Україні», який той зробив разом зі своїм колегою – Огненом Вукоєвичем – святкуючи перемогу над збірною Росії в чвертьфіналі ЧС2018.

Дисциплінарний комітет ФІФА виніс попередження Віді, оскільки організація розцінила його звернення як політичний жест.

Через тиск з боку ФІФА хорватська федерація звільнила Вукоєвича з посади помічника тренера збірної Хорватії та відрахувала зі складу делегації на ЧС-2018.

Окрім роботи з офіційною сторінкою ФІФА у Фейсбуку, українці активно поширюють відео, в якому світові лідери вживають слово «Слава Україні».

Посольство України у Великій Британії відреагувало на те, що у кількох британських топ-медіа гасло «Слава Україні» назвали «націоналістичним», пояснивши, що вираз має патріотичне значення на кшталт «Нехай живе Франція», «Нехай живе Королева».

***

11.07.2018

После ФИФА украинцы обвалили рейтинг «Газпрома» в Facebook

Украинские пользователи занизили рейтинг российской компании «Газпром» в соцсети Facebook (InternetUA).

Вечером 10 июля пользователи начали ставить компании оценку «1» с комментариями «Слава Украине» и «Слава Хорватии», и за несколько часов обрушили рейтинг до 1,5 звезд из максимальных пяти. После этого администраторы страницы отключили возможность оценки.

***

13.07.2018

«Врятуйте Сенцова!» Українці та іноземці штурмують сторінку Трампа у соцмережі

Напередодні зустрічі американського і російського президентів, українці та іноземці масово тегають у соцмережі Twitter-сторінку Дональда Трампа (Експрес).

Вони просять його посприяти звільненню українського режисера Олега Сенцова, який перебуває у російській колонії. «Дональде Трампе, нагадайте Путіну, що настав час звільнити Сенцова та всіх українців, які є заручниками Кремля», – йдеться в одному з повідомленнь, яке поширюють у мережі.

.@realDonaldTrump remind #Putin it's Time to #FreeSentsov & all the Ukrainians being held hostage by the Kremlin #SaveOlegSentsov #Sentsov #CrimeaIsUkraine #WorldCup #Trump #Pompeo #Bolton pic.twitter.com/YjlZSQ4hW2

***

18.07.2018

Майя Яровая

«Молитва за доступный общественный транспорт»: в украинском Facebook вирусится новый флешмоб

Прошло более трех лет после Фестиваля паники и истерики в Киеве, и вот украинцам подвезли новую «зраду». С 14 июля в Киеве в два раза подорожал проезд в общественном транспорте, а сегодня жители столицы собираются на «Молитву за снижение цен». Так называется созданное на днях Facebook-мероприятие, которое всего за стуки собрало более 1500 участников и еще больше интересующихся, число уже превысило 6000 пользователей и продолжает расти (AIN.UA).

«Достало, что цены на проезд растут, а денег ты больше не зарабатываешь? Нужно ездить на метро и троллейбусе, а теперь это удовольствие только для богатых? Приходи и молись с нами за снижение цен на проезд в общественном транспорте», – говорится в описании мероприятия.

Пользователи активно принимают участие в обсуждениях, комментируют и рекомендуют мероприятие своим друзьям, сочиняют шутки и мемы на тему подорожания проезда в столице. Новые посты появляются один за другим с интервалом в несколько минут.

Стоимость участия в мероприятии не указана, однако на его финансирование организаторы собирают пожертвования – 8 грн. Ровно столько отныне берут за проезд в столичных автобусах, трамваях, троллейбусах и метро.

По словам организатора Дмитрия Косинского, мероприятие было опубликовано 17 июля и получило значительный органический охват. С тех пор на ивент откликнулось более 8000 пользователей.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

11.07.2018
В ленте Facebook появится AR-реклама

Пользователи смогут взаимодействовать рекламой с помощью камеры мобильных девайсов. Одна из тестовых реклам с дополненной реальностью на Facebook от Michael Kors позволяет юзерам виртуально примерить очки. Sephora, NYX Professional Makeup, Bobbi Brown, Pottery Barn, Wayfair и King представят свою рекламу этим летом. Ранее лидером отрасли по использованию AR-рекламы был Snap. Apple также использует AR-технологию, поощряя разработчиков создавать контент с помощью своего ARKit. Более 80 млн людей в США ежемесячно исопльзуют AR, омтечает The Boston Consulting Group. Эта цифра должна достигнуть 120 млн к 2021 году (Marketing Media Review).

***

11.07.2018
Facebook закрывает второй проект дрона для раздачи интернета

Недавно Facebook свернул проект беспилотника Aquila, а теперь та же участь постигла дрон-вертолет Tether-tenna, который планировалось использовать в качестве базовой станции для обеспечения связи в чрезвычайных ситуациях.

Докладніше

***

10.07.2018
В Snapchat найдена скрытая функция покупок по фотографии

Мессенджер Snapchat, в котором люди могут обмениваться фотографиями и короткими видео, вскоре может предложить новую функцию – покупки на сайте Amazon с помощью камеры (IGate).

Исследователь приложений Исхан Агарваль нашел в Snapchat скрытый код для функции визуального поиска. Это позволит программе с помощью камеры идентифицировать объекты и штрих-коды, а при определении совпадения, перенаправлять пользователя на сайт крупнейшего онлайн-ритейлера Amazon.

Так, Snapchat уже имеет функцию распознавания музыки с помощью Shazam. Чтобы узнать, какая музыка звучит, достаточно зажать кнопку камеры на экране и Shazam начнет поиск. Все найденные песни можно отправлять в контакты Snapchat своим друзьям.

Кроме этого, в мессенджер встроен сервис для совершения покупок через

приложение, который можно было бы объединить с покупками через интерфейс камеры.

Пока ни в Amazon, ни в Snapchat не прокомментировали обнаруженную функцию.

***

11.07.2018

Бренды vs пользователи: что покупатели хотят шерить в сетях

Недавнее исследование Sprout Social, в ходе которого было опрошено 1,253 потребителей и 2,060 SMM-маркетологов в апреле и мае 2018 года, показал отличия между тем, что постят маркетологи в социальных медиа, и чего хотят покупатели от постов брендов. Больше всего пользователи ценят посты о скидках/распродажа (72 %) и посты с демонстрацией новых продуктов и услуг (60 %). Бренда же чаще всего шерят в сетях посты, которые могут чему-то научить (61 %) и посты, которые рассказывают истории (58 %) (Marketing Media Review).

***

11.07.2018

Facebook оштрафовали на 660 тысяч долларов за скандал с Cambridge Analytica

Из-за скандала с Cambridge Analytica социальная сеть Facebook получила максимально возможный штраф в размере 660 тыс. долларов. Об этом сообщает The Guardian (InternetUA).

«Facebook не смог обеспечить такую защиту, которую они должны соблюдать в соответствии с законом о защите данных. Штрафы нужны для наказания, но моя реальная цель – произвести изменения и восстановить доверие и уверенность в нашей демократической системе», – заявила комиссар по информации Элизабет Денхам.

Отмечается, что в первом квартале 2018 года Facebook зарабатывала 664 тыс. долларов каждые пять с половиной минут.

***

15.07.2018

Facebook будет разрабатывать чипы с искусственным интеллектом

Социальная сеть Facebook переманила к себе бывшего сотрудника Google, который до этого работал на Apple – они планируют использовать его знания для того, чтобы изготавливать собственные чипы с искусственным интеллектом. Шахрияр Рабиль проработал в Facebook девять лет (InternetUA).

Работу Facebook над чипами, которые оснащены ИИ, в последние несколько месяцев обсуждали издания о технологиях – в частности,

TechCrunch. Они отмечают, что это «смелое направление для компании», однако не уверены в целях Facebook. По всей видимости, это будут чипы для потребительских устройств, с помощью которых они будут оценивать поведение пользователей.

Создание собственных чипов, предположительно, позволило бы Facebook больше не пользоваться чипами другого американского производителя – Qualcomm, а также снизить расходы, пустив их на изготовление своих серверов, а не технологии NVIDIA. Так компания могла бы получить некоторое преимущество на рынке устройств – например, в работе над своей умной колонкой.

При этом, деятельность Рабиля включала в себя работу над чипами для потребительских устройств, в частности – над визуальным ядром Pixel 2, который совместил работу машинного интеллекта и камеры устройства.

Издание TechCrunch отмечает, что за последний год Google трудоустроил у себя несколько бывших сотрудников Apple для создания собственных инновационных процессоров, однако соперник компании решил поступать точно так же.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

7.07.2018
Гнітюча самотність: соцмережі руйнують психіку дітей

Все більша кількість дітей скаржаться на почуття ізоляції і самотності. Психологи вважають, що ситуацію погіршують соціальні мережі (Gazeta.ua).

«Майже 80 % консультаційних звернень припадають на дівчаток, багато з яких стверджували, що вплив соціальних мереж і порівняння себе з іншими користувачами Інтернету змушують їх відчувати себе все більш ізольованими. В соціальних мережах діти бачать, що друзі добре проводять час, відпочивають чи граються, і це їх засмучує, бо вони одинокі. Настрій погіршується і потім це впливає на успішність в закладах навчання. Як снігова лавина, депресія породжує нові проблеми», – повідомила засновник британської служби допомоги дітям і підліткам Естер Ранцен, повідомляє Independent.

Самотність удвічі підвищує ризик серцево-судинних захворювань. Науковці з Данії провели дослідження за участі 13 тис. осіб. Виявилося, що почуття самотності є передвісником передчасної смерті.

***

8.07.2018
Социальные сети намеренно вызывают зависимость

Инсайдеры из Кремниевой долины поделились информацией для нового документального фильма BBC, согласно которой, технологические компании используют различные трюки и уязвимости в человеческой психологии для вызывания зависимости от своих продуктов.
Докладніше

***

9.07.2018
Небезпечний смартфон: 11 причин вимкнути гаджет

У 21 столітті складно уявити життя без смартфона. Але все частіше в інтернеті з'являються історії про людей, які вирішили тимчасово відмовитися від гаджетів та соцмереж і влаштувати собі «інформаційний детокс».
Компанії-виробники девайсів підтримують ці тенденції.
Докладніше

***

17.07.2018
Американські вчені знайшли зв'язок між зловживанням соцмережами та розладом у підлітків

Чим більше підлітки сидять у соціальних мережах і дивляться відео в Інтернеті, тим більше шансів, що у них можуть розвинутися симптоми синдрому дефіциту уваги і гіперактивності (СДУГ). До такого висновку прийшли вчені з Університету Південної Каліфорнії в США.
Докладніше

Маніпулятивні технології

9.07.2018
Ирина Фоменко
Фейсбук проигрывает войну фейковым профилям

На сегодняшний день вопрос о фейковых профилях в социальных сетях стоит довольно остро. В Facebook, Instagram и Twitter очень много людей выдают себя за других, например, актеров, певцов, политиков и других известных деятелей для обмана обычных пользователей.
Докладніше

***

6.07. 2018

МІП звернулось до Facebook щодо блокування українських активістів та поширення російської пропаганди

Міністерство інформаційної політики України звернулося з листом до керівництва компанії Facebook у зв'язку з порушеннями соціальною мережею свободи слова українських користувачів, а також де-факто політикою сприяння поширенню фейкових новин і пропаганди державою-агресором Російською Федерацією та підконтрольними їй терористичними угрупованнями – т. зв. «Донецькою Народною Республікою» (ДНР) і «Луганською Народною Республікою» (ЛНР) (Міністерство інформаційної політики).

МІП звертає увагу, що в офіційних стандартах Facebook вказано, що спільнота не допускає присутності у соціальній мережі організацій та осіб, які займаються терористичною діяльністю, організованими ненависництвом, масовими чи серійними вбивствами. А українські органи державної влади визнають «ДНР» та «ЛНР» саме терористичними організаціями.

Міністерство інформаційної політики просить керівництво компанії унеможливити використання інструментарію Facebook як засобу обмеження свободи слова українських активістів, що протистоять гібридній війні, розв'язаній РФ, та натомість вжити оперативних і дієвих заходів щодо припинення функціонування в соціальній мережі сторінок та груп, діяльність яких суперечить стандартам спільноти, оскільки їхня діяльність має деструктивні наслідки для українського народу, а також для іміджу самої компанії.

***

9.07.2018

Ви виграли телефон: як шахраї з соцмереж кидають українців

Останнім часом українцям надходять повідомлення про те, що вони виграли приз (InternetUA).

Українців тероризують шахраї новою схемою розводу. Людям приходять повідомлення у соціальних мережах і месенджерах, де говориться, що вони стали переможцем у якійсь акції або їм нараховані гроші на покупку коштовного призу.

***

10.07.2018

YouTube решил выделить $25 млн на борьбу с фейковыми новостями

Видеохостинговая компания YouTube решила выделить $25 млн для борьбы с фейковыми новостями. Об этом сообщает The Hollywood Reporter

(InternetUA).

Отмечается, что после критики из-за продвижения дезинформирующего контента компания решила усовершенствовать свою платформу. Вместе с Google News YouTube решил способствовать распространению качественных новостных видео. Так, для поддержки глобальных новостных организаций компания готовы выделить $25 млн в виде грантов.

Как уточняется, планируется сотрудничество с новостными агентствами и экспертами, авторитетные источники новостей также получат поддержку.

***

10.07.2018

Французьке законодавство дозволить боротися з фейковими новинами на державному рівні

Парламент Франції ухвалив законопроект, який суттєво посилює юридичний механізм захисту демократичного життя від фейкових новин, а також розширює можливості протидії поширенню неправдивої інформації, зокрема в передвиборний період.

Докладніше

***

15.07.2018

Россию обвинили в разобщении американской нации через соцсети

Министр внутренней безопасности (МВБ) США Кирстен Нильсен заявила, что Россия пытается разобщить американцев через социальные сети. Об этом она рассказала 14 июля в Филадельфии на встрече с чиновниками, ответственными за проведение выборов в США.

Докладніше

***

16.07.2018

Поліція Чернігова викрила шахрайку, яка одурила довірливих громадян на 13 тисяч гривень

Жінка розмістила в соцмережі пост про збір коштів на нібито лікування матері. Небайдужі українці повірили зловмисниці і перерахували їй значні кошти (InternetUA).

До поліції звернулися жителі Чернігова і повідомили, що протягом кількох місяців жителька обласного центру розміщала в «Інстаграмі» повідомлення з проханням фінансової допомоги на нібито лікування матері. Насправді це виявилося неправдою.

Таким чином, шляхом обману зловмисниця заволоділа грошовими коштами громадян на загальну суму близько 13000 гривень. Лиходійка у

скоєному зізналася.

Інформація про подію внесена до Єдиного реєстру досудових розслідувань, відкрито кримінальне провадження за частиною 1 статті 190 Кримінального кодексу України (шахрайство) – карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років.

Триває досудове розслідування.

***

15.07.2018
Twitter заблокировал 2 аккаунта, связанные с российской разведкой

Социальная сеть Twitter заблокировала 2 аккаунта, которые связаны с 12 гражданами Российской Федерации (РФ), уличенными во вмешательстве в выборы в США. Об этом пишет Reuters (InternetUA).

Так, как сообщает издание, ссылаясь на руководство Twitter, учетные записи @DCLeaks_ и @Guccifer_2 заблокированы.

«Эти аккаунты были названы в обвинительном заключении 12 сотрудникам военной разведки РФ», – отметили в Twitter.

«Учетные записи были заблокированы из-за связи с сетью аккаунтов, которые ранее были заблокированы за нарушающую наши правила деятельность», – говорится в заявлении представителя Twitter.

***

17.07.2018
Ирина Фоменко
Как боты соцсетей могут обвалить ваши акции

В этом году ученые Zignal начали замечать «аномалии в данных»: посты неизвестных людей, получивших признание лидеров мнений, а также всплески активности по определенным темам.

Докладніше

***

18.07.2018
Ирина Фоменко
Facebook оказался замешан в фальсификации BREXIT

Избирательная комиссия Великобритании опубликовала результаты почти девятимесячного расследования по расходам на референдум Brexit и обнаружила, что официальная кампания Vote Leave нарушила закон, превысив расходы.

Докладніше

Спецслужби і технології «соціального контролю»

5.07.2018
Майя Яровая
Комитет нацбезопасности одобрил скандальный законопроект №6688 // Эксперты: это шаг к тоталитаризму

Скандальный законопроект №6688, которым, среди прочего, предлагается блокировать сайты на 48 часов без разрешения суда, 4 июля одобрили в Комитете по вопросам национальной безопасности и обороны.

Докладніше

***

8.07.2018
Працівницю дитячої лікарні засудили за антиукраїнські заклики в соцмережі

Лаборантку Кременчуцької дитячої лікарні засудили до іспитового строку терміном один рік. Жінка поширювала в соцмережі антиукраїнські матеріали (InternetUA).

З квітня 2015 до березня 2018 року вона розміщувала на власній сторінці у «ВКонтакте» заклики до антиконституційної зміни державного кордону та розповсюджувала їх серед інших користувачів. Зокрема, обвинувачена писала, що Донбас розташований на території Росії, а так звані «ДНР» та «ЛНР» – незалежні держави, що не входять до складу України.

Жінка визнала власну вину та уклала угоду зі слідством.

Суд визнав її винною за ч. 1 ст. 110 (Умисні дії, вчинені з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України, а також публічні заклики чи розповсюдження матеріалів із закликами до вчинення таких дій) Кримінального кодексу України та засудив до трьох років позбавлення волі, проте змінив основне покарання на рік іспитового строку. Крім того вона має сплатити 13,4 тис. грн за проведені експертизи.

***

9.07.2018
Ирина Фоменко
Твиттер наносит удар по ботам

С октября прошлого года Twitter вдвое больше заблокировал фейковых аккаунтов в рамках постоянной борьбы с поддельными учетными записями, в том числе ботами и интернет-троллями. Компания продолжает обеспечивать

контроль после президентских выборов в США в 2016 году, спровоцировавших скандалы, связанные с пропагандой, дезинформацией и преследованиями в социальных сетях. Усилия Twitter могут привести к снижению статистики использования сайта.

Докладніше

***

10.07.2018

В Европе обеспокоены законом Украины о блокировке сайтов

В Совете Европы заявили об угрозе свободе слова со стороны украинского государства из-за законопроекта «О внесении изменений в некоторые законодательные акты Украины относительно противодействия угрозам нацбезопасности в информационной сфере», который позволяет досудебное блокирование сайтов (InternetUA).

Об этом говорится в перечне уведомлений Совета Европы относительно угроз свободе слова.

В Совете Европы отметили, что ряд медиа-организаций оценили закон как попытку ввести цензуру в интернете и нарушить принципы приватности в интернете.

Как отмечается, украинская власть пока не отреагировала на озабоченность Совета Европы.

***

9.07.2018

Україна та ЄС координуватимуть дії для протидії загрозам втручання у вибори – Глава держави

Під час Двадцятого Саміту Україна – Європейський Союз його учасники обговорювали майбутні вибори в Україні та ЄС наступного року, повідомив Президент Петро Порошенко (Офіційне інтернет-представництво Президента України).

«Це останній Саміт перед дуже важливими виборами, як в Україні – парламентськими та президентськими, так і в ЄС наступного року», – зазначив Глава держави під час спільної прес-конференції з Президентом Європейської Ради Дональдом Туском та Президентом Європейської Комісії Жан-Клодом Юнкером за результатами Саміту.

«Без сумніву, Кремль спробує знову втрутитися, але цього разу ми будемо готові. Ми погодились координувати та вжити спільних заходів для протидії загрозам втручання будь-якого характеру, незалежно від того, чи це кампанія з дезінформації чи кібератаки», – сказав він.

***

10.07.2018

Facebook блокирует украинцев, пожаловавшихся на страницу FIFA

Социальная сеть начала временно блокировать аккаунты украинцев, которые участвовали во флешмобе на странице FIFA, отмечает biz.liga.net. Как написал редактор K750 Media Роман Судольский, он несколько минут не мог зайти, после чего Facebook предложил поменять пароль и начал процедуру подтверждения аккаунта: показывать списки последних действий, добавленных друзей, лайков и т.д. Отметим, FIFA уже удалила страницу с отзывами. Напомним, украинцы решили поддержать хорватских игроков, которые разместили видео после победы над Россией со словами «Слава Украины». Пользователи понизили рейтинг страницы FIFA в Facebook до 1,3 звезды. Ранее MMR спросил PR- и digital-экспертов, что делать бренду, в которой оказалась FIFA (Marketing Media Review).

***

11.07.2018

Россия капитулировала в войне с Telegram

Российские власти намерены отказаться от попыток полностью заблокировать мессенджер (InternetUA).

Об этом 10 июля, спустя несколько часов после своего назначения, заявил новый спецпредставитель президента РФ по цифровому развитию Дмитрий Песков, передает finanz.ru.

По словам Пескова, ранее возглавлявшего одно из направлений Агентства стратегических инициатив, сейчас, после трех месяцев усилий Роскомнадзора, наступил «идеальный момент» для того, чтобы начать контактировать с владельцами Telegram.

Можно найти решения, «которые будут допустимы для всех сторон этой ситуации и которые, с одной стороны, решат задачи безопасности, с другой стороны, не приведут к окончательному закрытию действия этого сервиса на территории РФ», – цитирует Пескова РИА Новости.

Он добавил, что сейчас существует «простор для таких договоренностей».

***

11.07.2018

СБУ і «Антонов» підписали меморандум щодо обміну даними про кібератаки в режимі реального часу

Служба безпеки України продовжує розширювати співпрацю з ключовими об’єктами критичної інфраструктури. СБУ для розбудови ефективної системи кібербезпеки держави підписала Меморандум з державним підприємством «Антонов» (InternetUA).

Документ має забезпечити обмін у режимі реального часу

технологічними даними щодо кіберінцидентів з використанням платформи MISP-UA. Фахівці спецслужби впенені, що дані з MISP-UA сприятимуть підвищенню захищеності державного підприємства стратегічного значення та сприятимуть ефективному реагуванню з боку СБУ та інших суб'єктів забезпечення кібербезпеки на атаки високого ступеня складності.

Довідково: Співробітниками Ситуаційного центру забезпечення кібербезпеки СБУ на базі платформи з відкритим програмним кодом MISP (MalwareInformationSharingPlatform), створено систему збору і обробки інформації щодо інцидентів кібернетичної безпеки та обміну технічними даними про ідентифікатори компрометації інформаційних систем об'єктів критичної інфраструктури між суб'єктами сектору безпеки в режимі реального часу. Ця платформа широко використовується в усьому світі, відповідає міжнародним стандартам ЄС та НАТО, застосовується основними міжнародними суб'єктами у сфері кібербезпеки FIRST, CIRCL, CiviCERT, NATO NCI Agency тощо.

***

11.07.2018
За что вас могут забанить в Фейсбуке?

В последнее время Facebook стала активно рассказывать о своем внутреннем устройстве – видимо, это ответ на критику, с которой столкнулась компания после новостей об утечке данных пользователей. Недавно администрация соцсети разъяснила, за какие публикации пользователей могут забанить.

Докладніше

***

11.07.2018
Facebook оштрафовали на £500,000 в Великобритании

Британское управление комиссара по вопросам информации выписало максимальный штраф руководству компании за два нарушения закона о защите информации в связи со скандалом с компанией Cambridge Analytica. Facebook не смог защитить информацию пользователей и не был прозрачен относительно того, как пользовательские данные собирались другими компаниями. Управление комиссара по информации также возбудит уголовное преследование для родительской компании SCL, которой принадлежала Cambridge Analytica. Напомним, Cambridge Analytica нелегально получила доступ к личной информации 87 миллионов пользователей Facebook. После скандала компания объявила о банкротстве и закрылась (Marketing Media Review).

***

12.07.2018

В России предложили сажать пользователей за отказ удалить информацию из Сети

Депутаты-единороссы предложили наказывать россиян вплоть до года лишения свободы за «злостный отказ» опровергнуть или удалить из Сети «незаконную информацию», то есть данные, признанные судом порочащими честь и достоинство, экстремистскими или вредными для детей.

Докладніше

***

11.07.2018

СБУ запобігла кібератаці на об'єкт критичної інфраструктури

Співробітники СБ України блокували спробу російських спецслужб провести кібератаку на мережеве обладнання товариства «Аульська хлороперелівна станція», яке є об'єктом критичної інфраструктури країни.

Докладніше

***

12.07.2018

Михаил Сапитон

Число ваших подписчиков в Twitter может уменьшиться. Причина – удаление подозрительных аккаунтов

Сервис микроблогов Twitter удалит заблокированные аккаунты из общего списка подписчиков, сообщается в корпоративном блоге. Счет идет на десятки миллионов учетных записей – в соцсети считают, что они ведут подозрительную активность. Вероятно, ранее аккаунты принадлежали реальным людям, которые потеряли над ними контроль и не сменили пароль по требованию компании (AIN.UA).

Twitter оценивает, что в результате изменений, средний пользователь потеряет 4 подписчика – однако для крупных аккаунтов количество будет значительно больше.

Общее количество подписчиков может сократиться примерно на 6 %, рассказал представитель Twitter в материале The New York Times. В январе издание выпустило нашумевшее расследование о небольшой компании из Флориды, которая занимается продажей фейковых подписчиков тысячам клиентов по всему миру. Накрутками пользовались политики, знаменитости, модели. Материал спровоцировал открытие расследований как минимум в двух штатах и подтолкнул Twitter к собственному аудиту.

С мая по июнь 2018 года Twitter заморозил около 70 млн подозрительных аккаунтов, уличенных в связях с российской «фабрикой троллей» во главе с Евгением Пригожиным, пишет Washington Post. Ему и еще 12 гражданам РФ

предъявлены официальные обвинения во вмешательстве в американскую политику со стороны министерства юстиции США.

Проблема захисту даних. DDOS та вірусні атаки

5.07.2018

Слежка за пользователями смартфонов ведется не совсем так, как мы думали

Согласно сообщению Gizmodo, команда исследователей обнаружила, что некоторые приложения для смартфонов тайно записывают происходящее на экране устройства и передают эту информацию.

Докладніше

***

5.07.2018

Михаил Сапитон

«Яндекс» проиндексировал Google Docs, доступные по ссылке. Как защитить информацию

Ночью с 4 на 5 июля «Яндекс» начал показывать в результатах поиска документы из сервиса Google Docs, доступ к которым распространялся по ссылке. Такие файлы может редактировать, просматривать или комментировать любой человек, получивший нужный URL – что в случае попадания в поиск означало общедоступность сведений.

Докладніше

***

5.07.2018

Фатальная компьютерная «бомба» вернулась

Эксперты в области кибербезопасности обнаружили, что в обновление Google Chrome вернулась техническая ошибка, позволяющая хакерам запугивать жертву с помощью «загрузочной бомбы». Об этом сообщает BleepingComputer (InternetUA).

Метод атаки «загрузочной бомбой» (или download-бомбой) позволяет запустить на интернет-странице сотни или тысячи загрузок, которые блокируют браузер. За несколько секунд процессор получает полную нагрузку, и компьютер зависает.

Мошенники часто используют этот трюк на своих фишинговых сайтах, ставя на заглушку страницы номер фальшивой технической поддержки или предложение оплатить услуги по разблокировке.

Ранее разработчики Google Chrome исправили уязвимость, которая

позволяла проводить подобные атаки. Как подтвердили пользователи, в нынешнем обновлении эта проблема вновь была замечена. Эксперт по безопасности Malwarebytes Джером Сегура (Jerome Segura), который провел масштабное исследование этого метода кибератак, заявил, что проблема «загрузочных бомб» может касаться не только браузера Google Chrome, но и Firefox.

***

9.07.2018

Смартфоны Xiaomi и Huawei шпионят за пользователями

Журналисты издания The Wall Street Journal выяснили, что около ста моделей смартфонов, выпускаемых Xiaomi и Huawei, поставляются с предустановленным приложением GMobi – оно предназначено для слежки за пользователями. Программа втайне собирает персональные данные владельцев, а компании используют их для демонстрации релевантных рекламных баннеров (InternetUA).

По данным WSJ, приложение присутствует во всех смартфонах вышеуказанных компаний, продаваемых в Китае, Камбодже, Мьянме, Бразилии и Индии. Изучив GMobi, специалисты по безопасности Upstream Systems выяснили, что программа в числе прочей информации передает на серверы IMEI и MAC-адрес устройства, а также данные о его местоположении.

На официальной странице GMobi указано, что сервис сотрудничает с более чем сотней компаний по всему миру, в числе которых есть Huawei и Xiaomi. Примечательно в этой ситуации то, что китайские гиганты полностью отрицают какую-либо связь с аналитической компанией. Объяснить, каким образом приложение Gmobi оказалось в прошивках для их устройств производители не смогли.

Глава аналитической компании Пол Ву рассказал WSJ, что у его команды уже несколько лет есть договоренность с вендорами по предустановке приложения на их смартфоны, хоть они это и отрицают. Ву добавил, что в деятельности компании нет ничего запрещенного – она подчиняется законам, регулирующим сбор, хранение и обработку персональных данных пользователей.

***

9.07.2018

21 млн пользователей сервиса Timehop стали жертвами утечки данных

Администрация сервиса Timehop, позволяющего находить опубликованные ранее материалы в соцсетях, сообщила о масштабной утечке данных. Инцидент произошел 4 июля текущего года и затронул 21 млн пользователей (InternetUA).

Утекшая база данных содержит порядка 4,7 млн телефонных номеров, а также имена пользователей и электронные адреса. По словам представителей сервиса, финансовые данные и контент соцсетей (переписка, фотографии, публикации и пр.) затронуты не были. Каких-либо свидетельств попыток неавторизованного доступа к учетным записям Timehop зафиксировано не было.

Кибератака была остановлена через 2 часа 19 минут с момента ее начала. Для ее осуществления злоумышленники завладели учетными данными для доступа к облачной среде Timehop, не защищенной с помощью двухфакторной аутентификации.

Еще в декабре прошлого года неизвестные авторизовались в облачной среде Timehop в качестве администратора и начали прощупывать почву. До 4 июля злоумышленники авторизовались подобным образом еще дважды.

В результате атаки все токены авторизации были аннулированы, и пользователи получили соответствующие уведомления. Для дальнейшего использования сервиса нужно заново подключить к нему учетные записи в соцсетях.

***

10.07.2018
Ирина Фоменко
Интернет вещей не подходит для шпионов

Безобидный обмен данными может привести к плачевным последствиям. Популярное фитнес-приложение и трекер физической активности Polar Flow определило месторасположение военного и государственного персонала, работающего на секретных объектах.

Докладніше

***

9.07.2018
Число вирусов для добычи криптовалют выросло в семь раз

За три месяца количество вирусов, которые заражают компьютеры и мобильные устройства для скрытой добычи криптовалют, увеличилось более чем в семь раз. Такой расчет сделали в компании McAfee (InternetUA).

По оценкам ее экспертов, к концу марта 2018 года зарегистрировано 2,9 млн образцов вредоносных программ для несанкционированного криптовалютного майнинга, тогда как к концу декабря 2017-го таких зловредов насчитывалось около 400 тысяч.

В исследовании говорится, что от вирусов-майнеров страдают как пользователи, так и компании. В частности, атаки пережили производитель электромобилей Tesla и страховая компания Aviva. Они не несут прямых материальных потерь, однако работа их компьютерных систем может

значительно замедлиться из-за нехватки мощностей, занятых вирусом.

Исследователи отмечают, что помимо киберджекинга (скрытое использование компьютера или другого устройства для криптомайнинга в фоновом режиме) еще одной серьезной угрозой становится кража криптовалют при помощи хакерских атак. Так, известная кибергруппировка Lazarus организовала полномасштабную атаку, которая получила название HaoBao. На компьютеры пользователей, имевших неосторожность открыть приложение из полученного электронного письма, скрытно устанавливается программа. Эта программа отслеживает майнинг пользователей и их операции с криптовалютами, сообщили в McAfee.

***

9.07.2018

Функция предупреждений Firefox о вирусах в загружаемых файлах работает некорректно

В Firefox предусмотрена интересная функция – браузер автоматически отмечает загрузку из интернета вирусов и другого вредоносного ПО. Несмотря на очевидную пользу, данная функция не всегда работает корректно.

Докладніше

***

9.07.2018

Хостинг-провайдер Domain Factory предупредил об утечке данных клиентов

Немецкий хостинг-провайдер Domain Factory сообщил об утечке информации, в результате которой были скомпрометированы данные клиентов компании, включая имена, пароли, физические и электронные адреса, номера телефонов, даты рождения, а также IBAN и BIC коды (InternetUA).

Об инциденте стало известно после публикации на форуме Domain Factory заявления атакующего, утверждавшего, что ему удалось скомпрометировать системы компании и получить доступ к сведениям. По его словам, мотивом атаки стал тот факт, что Domain Factory не заплатила ему деньги.

Как предполагается, злоумышленнику удалось получить доступ к информации путем эксплуатации варианта уязвимости DirtyCow. По имеющимся данным, инцидент произошел 28 января 2018 года, однако известно о нем стало только в начале июля.

Руководство компании призвало пользователей изменить свои учетные данные для аккаунтов Domain Factory как можно скорее. Кроме того, в качестве меры предосторожности компания порекомендовала установить новые пароли для MySQL, SSH, FTP и Live CD, поскольку в теории из-за утечки данных сайты клиентов также могут быть скомпрометированы.

***

10.07.2018

«Доктор Веб»: троянец-майнер загружается вместо обновления программ

Вирусописатели применяют различные методики распространения вредоносных программ. Среди них особо следует отметить использование злоумышленниками стандартного механизма обновления приложений. Именно так распространялся нашумевший троянец-шифровальщик Trojan.Encoder.12544, известный под наименованиями Petya, Petya.A, ExPetya и WannaCry-2, а также бэкдор BackDoor.Dande.

Докладніше

***

10.07.2018

Android-смартфоны поставляются с предустановленными вирусами

Тем, кто хочет приобрести бюджетный Android-смартфон стоит задуматься, так как в некоторых моделях были обнаружены вредоносные программы. Эта информация поступила от компании Upstream, занимающейся безопасностью онлайн-транзакций (Украинский телекоммуникационный портал).

По словам сотрудников Upstream, некоторые дешевые Android-смартфоны, продающиеся в Бразилии, Египте и в некоторых странах Южной Африки, содержат вирусы, способные украсть данные владельцев гаджетов и даже их деньги.

Предустановленные программы подключаются к неизвестным серверам, расположенным в Азии, и отсылают туда конфиденциальные данные пользователей. Также они подключают владельцев устройств к платным премиум-сервисам без их ведома.

Какие именно устройства подвержены угрозе, неизвестно. Ранее The Wall Street Journal называла лишь один смартфон с предустановленными вирусами, разработанный в Китае.

Это – Singtech P10. Стоит отметить, что на этом гаджете установлено программное обеспечение рекламной фирмы GMobi.

Самое страшное, что идентичный софт часто устанавливается на Huawei, Xiaomi и другие популярные китайские смартфоны, продающиеся на востоке.

***

10.07.2018

Хакеры подписывали вредоносное ПО сертификатом D-Link

Специалисты ESET обнаружили новую киберкампанию, в которой

используются сертификаты для подписи кода, украденные у компании D-Link (Компьютерное Обозрение).

Вредоносная кампания была зафиксирована ESET после обнаружения нескольких подозрительных файлов. Они были подписаны действительным сертификатом D-Link Corporation. Тот же сертификат использовался в легитимном ПО D-Link.

Убедившись во вредоносности файлов, ESET сообщила о проблеме в D-Link. Скомпрометированный цифровой сертификат был отозван компанией 3 июля.

В ходе исследования в ESET нашли также вредоносные образцы, подписанные сертификатом другой тайваньской технологической компании – Changing Information Technology Inc., которая специализируется на продуктах для безопасности. Данный сертификат отозван 4 июля 2017 г.

С помощью украденных сертификатов распространялись два семейства вредоносных программ: бэкдор для удаленного управления зараженным компьютером Plead и связанный с ним инструмент для сбора паролей, сохраненных в Google Chrome, Internet Explorer, Microsoft Outlook и Mozilla Firefox.

По мнению экспертов, за атакой стоит кибершпионская группа BlackTech, атакующая цели в Восточной Азии. Компрометация технологических компаний демонстрирует высокую квалификацию данной группы.

Использование украденных цифровых сертификатов – распространенный способ маскировки. Сертификаты позволяют вредоносным программам выглядеть как легитимные и обходить защиту, не вызывая подозрений. Метод реализован, в частности, в 2010 г. в Stuxnet – первом кибероружии, ориентированном на критическую инфраструктуру.

***

11.07.2018

ICO-проекты в числе наиболее популярных целей киберпреступников

Киберпреступники продолжают активно использовать ажиотаж вокруг цифровых денег: кроме взлома криптовалютных бирж, эксплуатации уязвимостей в смарт-контрактах и использования зловредов-майнеров, мошенники прибегают и к классическим методам социальной инженерии.

Докладніше

***

11.07.2018

Ирина Фоменко

Предпочитаете Gmail? Тогда прочтите это

В первых числах июля появились отчеты, подтверждающие, что

сторонние разработчики приложений могли читать электронные письма, принадлежащие миллионам учетных записей Gmail. Сегодня Конгресс требует от Google ответов на множество вопросов, связанных с конфиденциальностью.

Докладніше

***

11.07.2018

CNN рассказал о возможной связи Mail.ru со скандалом в Facebook

Российская Mail.ru Group может быть причастна к скандалу со злоупотреблением данными Facebook, передает CNN. Пока ни о каких конкретных нарушениях не сообщается.

Докладніше

***

12.07.2018

WhatsApp предупредил пользователей об опасности

В официальном блоге WhatsApp появилось сообщение, в котором пользователям настоятельно советуют быть внимательными, когда они пересылают своим контактам чужие сообщения (InternetUA).

По всей видимости, речь может идти о распространении фальшивых новостей, которые пользователи массово рассылают друг другу в ряде стран. Фейки привели к серьезным конфликтам в Индии.

Для того чтобы понять, было ли сообщение написано знакомым, а не посторонним человеком, в мессенджере была реализована новая пометка – «пересланное сообщение» (forwarded). Она будет сопровождать сообщения, которые пользователю были пересланы от других людей. Таким образом можно будет быстро понять, пишет пользователь от своего имени или пересылает чужой текст.

***

12.07.2018

Пользователей Android атаковал опасный вирус

Исследователи безопасности из IBM X-Force обнаружили опасный троян Anubis, скрывающийся в приложениях из Google Play. Об этом эксперты рассказали в своем блоге (InternetUA).

По данным специалистов, киберпреступной группировке удалось спрятать вредоносное ПО в десятке программ для смартфонов под управлением Android. Вирусы были замаскированы под интернет-магазины, финансовые помощники и автомобильные приложения.

После загрузки зараженной программы на устройство Anubis под видом встроенного антивируса Google Protect и запрашивал права для сканирования

действий пользователя. После этого троян мог делать скриншоты экрана, пока владелец телефона вводил личные данные в банковских приложениях и электронных кошельках.

Разработчики вируса регулярно модернизировали его возможности и изменяли код, чтобы алгоритмы безопасности Google Play их не обнаружили. Специалисты заявили, что Anubis предназначался для пользователей из Турции, однако конфигурация вредоносного ПО показывает, что вирус может распространиться и в другие страны.

Сотрудники IBM X-Force отправили компании Google результаты исследования, чтобы модераторы удалили опасные приложения из магазина.

***

13.07.2018

К популярной бесплатной утилите для удаленного доступа прилагался троян

Компания ESET предупреждает о компрометации официального сайта Ammyy Admin – популярной бесплатной программы для удаленного доступа к компьютеру. 13-14 июня злоумышленники использовали сайт для распространения вредоносного ПО под видом легитимного софта.

Докладніше

***

15.07.2018

Аккаунты украинцев воруют, а затем продают в интернете

Украинцы не заморачиваются сохранностью своих интернет профилей – злоумышленники с легкостью уводят у них личные аккаунты и даже целые онлайн-магазины у мелкого e-commerce. В зоне риска находятся как пользователи популярных соцсетей и досок объявлений, так и мелкие предприниматели, реализующие товары с помощью крупных маркетплейсов.

Докладніше

***

17.07.2018

Яндекс злив банківські дані мільйонів

Скани паспортів, дані про банківські платежі, інформація про квитки на літаки та поїзди стали доступні в пошуковій видачі «Яндекса» (InternetUA).

Повідомляється, що кожному користувачеві пошуковика «Яндекс» стала доступна інформація громадян з сайтів Сбербанку і ВТБ, департаменту транспорту Москви і агрегатора квитків Trip.com.

Самі ж представники «Яндекса» пояснили, що власник сайту чи вебмастер можуть закрити інформацію про документи – пошукова система

видає документи, які не заборонені за допомогою спеціального файлу.

В Сбербанку у зв'язку з даною ситуацією йде розгляд. Однак банк підкреслив, що даних, які можуть завдати шкоди організації або клієнтам, тут немає, проте особисті дані користувачів все ще доступні будь-якому бажаючому.

***

17.07.2018

Произошла утечка учетных данных пользователей Mega

Несколько тысяч пользователей новозеландского облачного хранилища Mega стали жертвами утечки учетных данных. Исследователь безопасности Патрик Уордл (Patrick Wardle) из компании Digita Security обнаружил в Сети текстовый файл, содержащий более 15,5 тыс. электронных адресов и паролей, а также списки файлов пользователей. Об этом сообщило издание ZDNet (InternetUA).

По словам специалиста, текстовый файл был найден в июне текущего года. Документ был загружен на сайт VirusTotal несколькими месяцами ранее пользователем, предположительно находящимся на территории Вьетнама.

Ряд пользователей подтвердили подлинность адресов электронной почты, паролей и названий файлов, содержавшихся в документе. Как отметил владелец агрегатора утечек данных Have I Been Pwned Трой Хант (Troy Hunt), системы Mega не были скомпрометированы, так как данные, скорее всего, были похищены со сторонних сайтов. 98 % адресов электронной почты, содержавшихся в файле, уже были внесены в базу данных Have I Been Pwned.

По словам представителей Mega, обнаруженный список был составлен с помощью метода credential stuffing (автоматизированной проверки похищенных учетных данных с помощью украденных баз данных). Утечка затронула порядка «0.0001 % от 115 млн пользователей Mega».

В настоящее время неясно, кто является автором списка и каким образом данные были собраны. Представители Mega пообещали добавить двухфакторную аутентификацию на сайт для того, чтобы избежать подобных проблем в будущем.

***

17.07.2018

Крупнейшая клиническая лаборатория США стала жертвой кибератаки

Неизвестные хакеры взломали сеть крупнейшей диагностической лаборатории США LabCorp и попытались получить доступ к конфиденциальным медицинским записям миллионов клиентов компании, сообщает издание DailyMail со ссылкой на осведомленные источники (InternetUA).

По данным ресурса, в результате инцидента, произошедшего в минувшие выходные, вся компьютерная сеть LabCorp на территории США была отключена. В настоящее время технические специалисты компании пытаются восстановить работу системы.

Как утверждают представители LabCorp, «нет свидетельств неавторизованного перемещения или использования данных», однако, по словам собеседника издания, на данный момент нельзя утверждать, что данные не были скомпрометированы. Оценка реального масштаба утечки может занять несколько недель, отметил источник.

Компания уже проинформировала правоохранительные органы об инциденте. В настоящее время проводится расследование.

LabCorp (Laboratory Corporation of America Holdings) – американская медицинская корпорация, осуществляющая деятельность в сфере здравоохранения. Управляет сетью специализированных клинических лабораторий, присутствует на территории разных стран мира, включая Пуэрто-Рико и Канаду.

***

17.07.2018

YouTube запустил инструмент для поиска копий оригинальных видео

Загружая чужие видео на свои каналы на YouTube, мошенники тем самым наживаются на чужом труде. У владельцев авторских прав на такие ролики уже есть несколько инструментов для защиты контента от копирования, но теперь компания запустила ещё один. Он автоматически сканирует каждое новое видео и проверяет его на идентичность уже загруженным в сервис роликам (InternetUA).

Стоит отметить, что инструмент, получивший название Copyright Match, работает только с целыми видео, но не с отдельными их частями. YouTube также отмечает, что настоящий автор должен загрузить ролик в сервис первым, поскольку система определяет скопированный контент именно по времени его добавления.

Когда инструмент находит копию видео, автору предлагается несколько вариантов действий. Можно либо связаться с человеком, который загрузил ролик, и попробовать разобраться с проблемой самостоятельно, либо попросить сотрудников YouTube удалить копию.

По своей сути новый инструмент очень похож на программу Content ID, в которой хранятся цифровые отпечатки – образцы контента, загруженные правообладателями. Тем не менее, компания делает акцент на том, что новинка пригодится исключительно для поиска несанкционированных копий. Content ID, в свою очередь, предназначена для владельцев авторских прав на музыку и музыкальные клипы, трейлеры и записи выступлений.

***

18.07.2018

В Бразилии задержали хакеров за взлом смартфонов соратников президента

В Бразилии полиция задержала четырех человек, которых подозревают в хакерских атаках на смартфоны политиков, в том числе президента страны Мишеля Темера (InternetUA).

Четыре человека задержаны в Бразилии по подозрению в хакерских атаках на смартфоны известных политических деятелей, в том числе ближайших соратников президента Мишель Темера. Об этом сообщает телеканал Globo.

Согласно его данным, в числе пострадавших оказались 25 человек, в том числе глава гражданской канцелярии президента Элисеу Падилья, секретарь по делам правительства Карлуш Марун, а также бывший министр социального развития Озмар Терра. После взлома мобильных устройств хакеры получали доступ к контактам политиков и под разными предлогами начинали просить денег у их знакомых. Многие из тех, с кем общались преступники, не решались отказать собеседникам, которых считали влиятельными чиновниками. Поэтому злоумышленники легко получали банковские переводы на запрошенные суммы.

По данным правоохранительных органов, в целом участники группировки смогли обогатиться на 76 тыс. реалов (около 20 тыс. долларов). Сейчас следователи пытаются установить, успели злоумышленники продать кому-нибудь конфиденциальную информацию со смартфонов чиновников.

***

18.07.2018

Студентів техвишу викрили у поширенні шкідливої програми для прихованого майнінгу криптовалют

Вірус вражав комп’ютер жертви, після чого без дозволу власника ПК, використовував потужності процесора для віддаленого майнінгу криптовалют. Наразі обом молодикам оголошено про підозру.

Докладніше

***

18.07.2018

Детские смарт-часы позволяют следить за своими владельцами

Пользователь портала Pikabu под псевдонимом dinikin обнаружил в детских смарт-часах Fixitime 3, произведенные компанией Elari, опасную уязвимость, позволяющую злоумышленнику следить за владельцем устройства (InternetUA).

По словам пользователя, он проанализировал трафик устройства и обнаружил возможность добавлять владельцев других часов в свое мобильное приложение.

Он также добавил, что данная уязвимость затрагивает все часы, произведенные китайской компанией Wherecom. Dinikin уведомил производителя о проблеме, однако, в настоящее время проблема остается неисправленной.

Помимо этого, dinikin выяснил местоположение серверов, на которые отправляются данные с устройства.

«Личные данные пользователей отправляются на китайский сервер и что хуже всего, вендор не имеет никакого контроля над этими данными. Это и не удивительно, ведь в мобильном приложении нет никакого лицензионного соглашения, а соответственно не прописано, куда передаются ваши личные данные и кто за это будет отвечать», – отметил он.

***

18.07.2018

Хакер взломал 13 iPhone высокопоставленных лиц

Компания Cisco Talos, занимающаяся проблемами компьютерной безопасности, сообщила, что ей удалось обнаружить вредоносное ПО, при помощи которого были взломаны 13 iPhone высокопоставленных лиц Индии.

Докладніше

***

18.07.2018

Мошенники выманивают деньги у клиентов крупного украинского банка

Специалисты кибербезопасности ПриватБанка сообщили о появлении в Украине новой мошеннической схемы с использованием поддельных писем о «случайном» переводе денег и поддельных сайтов, внешне напоминающих веб-сайт Приват24 (InternetUA).

По данным специалистов банка, уже зафиксированы случаи, когда клиентам через различные каналы коммуникаций (мессенджеры, электронную почту) приходит сообщение о пополнении карты неизвестным лицом на несколько тысяч гривен. Далее мошенники предлагаю перейти по ссылке на фальшивую квитанцию с фишинговым сайтом Приват24.

ПриватБанк предупреждает своих клиентов не открывать такие сообщения от мошенников и не реагировать на даже самые заманчивые сообщения о неожиданных денежных переводах. Также ни в коем случае нельзя вводить свои логин и пароль на поддельных банковских сайтах. Настоящий Приват24 находится только по адресу www.privat24.ua.

***

18.07.2018
Россия имела доступ к украденным из Facebook личным данным

Член британского парламента от Консервативной партии Дамиан Коллинс заявил, что у России и других стран был доступ к украденным личным данным миллионов пользователей социальной сети Facebook. Об этом он сказал телеканалу CNN (InternetUA).

Ранее в Facebook заявляли об утечке данных 87 млн пользователей, в которой обвинили британскую компанию по сбору и анализу данных Cambridge Analytica.

По словам Коллинса, специалисты офиса уполномоченного по информации установили, что к украденным личным данным имели доступ люди из России и других неназванных стран.

«Я думаю, что в данный момент мы хотим понять, кем были эти люди и какой доступ у них был. Фактически, мы хотим понять, могли ли они присвоить часть этих данных и использовать их в своих целях», – сказал парламентарий.

ДОДАТКИ

Додаток 1

9.07.2018
WhatsApp получил поддержку самой долгожданной функции

Мессенджер WhatsApp вот уже как много лет является наиболее популярным среди всех аналогов, а с недавних пор он вообще стал самым распространенным средством для общения в мире, потому как база его активных пользователей, постоянно обменивающихся какими-то сообщениями, превысила отметку в 1,5 млрд человек (Украинский телекоммуникационный портал).

Данному сервису сложно развиваться из-за Viber и Telegram, в которых есть некоторые уникальные возможности, поэтому разработчики решили начать копировать функционал. 9 июля 2018 года WhatsApp получил поддержку самой долгожданной функции, от которой все без ума.

Теперь при помощи данного сервиса можно не только совершать голосовые звонки, обмениваться сообщениями и делать все в таком духе, но еще и читать разного рода новости от множества источников.

Все благодаря тому, что разработчики наконец-то выпустили обновленную версию мессенджера, в которой появилась поддержка специальной функции, позволяющей преобразовать групповой чат в канал.

Теперь, начиная с версии WhatsApp 2.18.81, у пользователей есть возможность создать групповой чат, а затем преобразовать его в канал, в

котором публиковать какой-либо контент могут лишь его администраторы.

Для этого необходимо открыть группу, будучи ее администратором, после чего зайти в раздел «Данные группы» и нажать на кнопку «Настройки группы». В появившемся списке следует выбрать настройку «Только администраторы».

После этого в группе публиковать сообщения смогут только администраторы, то есть люди с таким статусом. Все остальные автоматически становятся не участниками беседы, а читателями.

Поддержка каналов уже давно есть в Telegram, а несколько месяцев назад она появилась в Viber. Миллионы людей ждали появления такой возможности в WhatsApp, потому как она расширяет функциональные возможности, позволяя использовать мессенджер не только для общения, но еще и для получения информации от каких-либо источников.

(вгору)

Додаток 2

11.07.2018

Facebook закрывает второй проект дрона для раздачи интернета

Недавно Facebook свернул проект беспилотника Aquila, а теперь та же участь постигла дрон-вертолет Tether-tenna, который планировалось использовать в качестве базовой станции для обеспечения связи в чрезвычайных ситуациях (Украинский телекоммуникационный портал).

Причем от идеи отказались всего лишь через несколько месяцев после ее презентации.

Проект Tether-tenna был представлен на конференции разработчиков F8 весной прошлого года.

Суть предложения состояла в создании «привязанного» вертолета, который используется для создания временной базовой станции в случаях разрушения основной инфраструктуры из-за стихийного бедствия или при необходимости обеспечить связью какое-либо мероприятие.

Специалисты Facebook проектировали для своего дрона антенную часть, а сам вертолет был построен на базе разработки стартапа Everfly, созданного компанией Otherlab.

Питание и сигнал на вертолет подается по кабелю с наземной станции, что позволило довести время эксплуатации системы до 24 часов. А в планах компании было заявлено увеличение срока использования базовой станции до «недель или месяцев».

Во всех отношениях проект Tether-tenna был проще, чем Aquila, поскольку имел «привязку» к земле. Но компания закрыла и его. Представитель Facebook сообщает, что Tether-tenna рассматривался, как концептуальный проект.

Группа из Otherlab, которая работала над проектом FB, пыталась расширить применение этой технологии на коммерческие

телекоммуникационные проекты, но не смогла получить финансирование и прекратила работы.

Эксперты считают, что отказ от Tether-tenna и Aquila свидетельствует о том, что в Facebook не хотят экспериментировать с авиационной частью.

Косвенно это подтверждается сообщением представителя компании Елла Магвайера, который сообщал, что FB готов сотрудничать с производителями высотных авиационных систем, например, с Airbus. Это позволит специалистам Facebook сфокусироваться на более знакомых вещах.

(вгору)

Додаток 3

8.07.2018

Социальные сети намеренно вызывают зависимость

Инсайдеры из Кремниевой долины поделились информацией для нового документального фильма BBC, согласно которой, технологические компании используют различные трюки и уязвимости в человеческой психологии для вызывания зависимости от своих продуктов. Мы давно обсуждаем тему зависимости от современных технологий. Возможно, для этого есть некоторые основания (InternetUA).

Согласно сообщению, Facebook, Snapchat, Twitter и другие компании намеренно разрабатывают интерфейс своих продуктов таким образом, чтобы он вызывал у людей привыкание и заставлял тратить на социальные сети больше своего времени.

Аза Раскин, создатель бесконечной прокрутки, говорит, что по страницам социальных сетей будто рассыпан визуальный наркотик, к которому пользователи привыкают все больше и больше.

Бывший руководитель Jawbone и Mozilla подтверждает, что за каждым элементом интерфейса стоят тысячи инженеров и компании, которые изучают привычки людей и их реакцию на те или иные элементы. От этого зависит все, включая цвет кнопки «like».

Бывший инженер Facebook Сэнди Паракилас, который покинул компанию в 2012 году, рассказал BBC, что руководство социальной сети полностью осознает, что все их действия направлены на выработку привыкания у людей. Бизнес-модель социальной сети состоит в том, чтобы заставить людей тратить на нее как можно больше своего времени, после чего Facebook продает это время рекламодателям.

Вице-президент Facebook по партнерским связям и продуктам сказал BBC следующее: «Мы работаем со сторонними лицами, которые изучают привычные формы поведения людей на нашей платформе и в Интернете, и пытаются понять, существуют ли элементы, которые приносят вред людям».

Пресс-секретарь Facebook рассказал Business Insider, что намерения компании самые лучшие: «Обвинения, возникшие в процессе создания BBC Panorama, неточны. Facebook и Instagram были предназначены для того, чтобы

связать людей с их друзьями, семьей и тем, что им нужно. Продукты могут связать вас с любимыми людьми, которые живут далеко или присоединить к сообществу людей, которые разделяют ваши интересы и поддерживают то, что для вас важно. Именно эта цель лежит в основе каждого дизайнерского решения, и ни на одной стадии приоритетом не становится вызывание привязанности».

Документальный фильм BBC Panorama транслируется в Великобритании. В нем рассказывается не только о Facebook, но и о Snapchat с Twitter. Создатель Snapchat уже заявил в адрес BBC, что его компания не использует визуальные трюки. В Twitter отказались от дачи комментариев.

(вгору)

Додаток 4

9.07.2018

Небезпечний смартфон: 11 причин вимкнути гаджет

У 21 столітті складно уявити життя без смартфона. Він допомагає підтримувати зв'язок з родиною і друзями, підказує, де найближчий стоматолог, допомагає не заблукати і знайомить з майбутнім чоловіком. Однак у бочці меду є ложка дьогтю (Свідок).

Все частіше в інтернеті з'являються історії про людей, які вирішили тимчасово відмовитися від гаджетів та соцмереж і влаштувати собі «інформаційний детокс».

Компанії-виробники девайсів підтримують ці тенденції.

Apple додала в операційну систему функції, які допоможуть зменшити використання гаджетів. За словами розробників, набір інструментів Digital Health дозволяє контролювати час, проведений за пристроєм та окремими додатками.

Нова операційна система Android також показує, скільки часу користувач витратив на використання того чи іншого додатка, скільки разів за день розблокував смартфон, скільки отримав повідомлень.

Функція App Timer дозволяє встановити ліміт часу на використання кожної програми. Функція Wind Down вимикає повідомлення. Опція Night Light вмикає чорно-білий режим дисплея, який нагадує, що пора спати. Функція Shush переводить смартфон в режим «не турбувати», коли користувач його перевертає.

Більшість людей сприймають смартфон як частину себе. Щоб поставити таким людям «діагноз», придумали термін номофобія (від англ. No mobile phone) – страх залишитися без свого смартфона.

За даними The Atlantic, сучасні підлітки, так звані міленіали і покоління Z, менше спілкуються, менше проводять часу в компаніях і навіть менше сплять. Усе це – через наявність у їх житті смартфонів.

З дорослими теж не все добре. Вранці вони насамперед перевіряють пошту, а у відпустці їх хвилює наявність Wi-Fi в номері готелю. Згідно з

дослідженнями, постійне використання смартфона може негативно позначитися на здоров'ї.

Вага. Люди стали більш ледачими ще з появою комп'ютерів. Коли ж «комп'ютер» опинився в кишені, все значно погіршилося.

Не потрібно йти в магазин – можна замовити доставку продуктів. Не обов'язково заходити до колеги в сусідній кабінет – можна написати в месенджер. Раніше для цього доводилося рухатися. Зараз фізична активність зводиться до того, щоб доїхати на роботу і з роботи, що часто призводить до ожиріння.

Спина. Причиною болю в спині, яку часто не здатні визначити лікарі, може бути смартфон. Постійно опускаючи голову, щоб подивитися на телефон, людина збільшує навантаження на спину. Також погіршується постачання крові до мозку, що призводить до головного болю і підвищеної стомлюваності.

Зір. Якщо комп'ютер негативно впливає на зір, то смартфон – ще більший ворог зору. Приклад – спроба розгледіти дрібний шрифт у напівтемному вагоні метро. Читати із смартфона офтальмологи не рекомендують.

Слух. Навушники не завжди забезпечують щільний контакт з вухом, і людям доводиться збільшувати гучність. Це призводить до індукованої втрати слуху – процесу, коли складно розібрати мову, особливо при наявності фонового шуму.

Сон. Світло екрана, від якого неможливо відірватися перед сном, негативно позначається на відпочинку. Світло змушує мозок думати, що ще день, і виробляти мелатонін. Це призводить до безсоння і тривожного сну. З 1991 року по 2015 рік кількість підлітків, які не досипають, зросла на 57 %.

Нестача сну може стати причиною ожиріння, підвищеного тиску і депресії.

Відносини. Романтичні і дружні стосунки можуть постраждати через гаджети. Доведено, що люди гірше концентруються на бесіді, якщо поруч лежить смартфон. Це може призвести до непорозуміння і конфліктів.

В останні роки підлітки стали рідше ходити на побачення. Навіщо витрачати час і кудись іти, якщо можна поспілкуватися по телефону?

Стрес. Повідомлення, звуки і вібрація смартфона підвищують рівень стресу.

Люди бояться пропустити важливі дзвінки або смс і постійно здригаються від вібрації. Оксфордський словник навіть ввів термін Fomo (від англ. Fear of missing out), який означає страх втратити інформацію. Люди, які страждають цим розладом, «живуть» у мережі, боячись пропустити щось важливе.

До слова, 89 % американських студентів відчувають «фантомні» вібрації, а 86 % американців постійно перевіряють пошту і соціальні мережі.

Депресія. Використання смартфона для перевірки соцмереж може призвести до депресії. Небезпечні і самі соціальні мережі: люди бачать створені іншими людьми ілюзії, створюють кращу копію себе і починають у неї вірити.

Вийшовши з мережі, людина бачить невідповідність реального і

віртуального світів, що призводить до закономірного рішення проводити у мережі більше часу. Зростає число підлітків, які відчувають себе покинутими і самотніми.

Пам'ять. Замість виконання розумових процесів люди передають їх цифровому помічнику. У підсумку, якщо раніше людина знала номери телефонів близьких і друзів напам'ять, могла продекламувати кілька віршів і назвати основні дати історії, то зараз в цьому нема необхідності.

Учені вважають, що водії, які користувалися навігатором, гірше запам'ятовували поїздки і не могли їх повторити без допомоги гаджетів. Люди, які знімали в музеях, пам'ятали менше, ніж ті, які не робили фото.

Рівень IQ. Негативно впливає смартфон і на інтелект. Ті, хто постійно стежать за повідомленнями і дзвінками, показали зниження рівня IQ на десять балів, що удвічі перевищує наслідки вживання марихуани.

Аварії. Збільшення кількості смартфонів призвело до збільшення частоти їх використання і, відповідно, до зростання числа аварій на дорогах. Раніше аварії траплялися через те, що водії говорили по телефону. Зараз вони просто на нього відволікаються, бо не вимикають сповіщення.

Це стосується і пішоходів, які дивляться на смартфон, а не навкруги.

Щоб врятувати себе треба – проаналізувати кількість часу, яка приділяється смартфону. Це можна зробити за допомогою опцій операційних систем Android або iOS 12. Остання вийде у вересні 2018 року.

Якщо смартфон не підтримує Android P, а нову операційну систему Apple чекати не хочеться, є низка додатків. Checky покаже, скільки разів за день людина розблокувала телефон, а BreakFree підрахує час роботи з тим чи іншим додатком. Програми підходять і для Apple, і для Android.

Поміняти розумний телефон на «нерозумний». Можливо, Nokia 1100, яка лежить у шафі з 2007 року, чекала саме цієї нагоди.

Кумедно, але тенденція переходу на «нерозумні» телефони з'явилася у Кремнієвій долині. Творці додатків, які спричиняють звикання, використовують звичайні телефони, щоб не відволікатися від роботи.

Зробити розумний телефон «дурнішим». Перейти на старий телефон зможуть не всі. Не дуже зручно носити ще й камеру, калькулятор, плеєр, блокнот і паперову карту, які раніше «поміщалися» в телефоні. Бракує сил, щоб відмовитися від цього дива техніки? Тоді можна урізати його функціонал.

Для початку – відключити повідомлення.

Буде трохи сумно дивитися на екран і бачити тільки час, але згодом це пройде.

Також варто поставити часові рамки для перевірки пошти, наприклад, раз на 30 хвилин. Потім можна збільшувати цей проміжок до 45 хвилин, до години і більше.

Крім того, можна вмикати режим «політ» або вимикати Wi-Fi під час обіду, тренування та їзди за кермом. Це допоможе не відволікатися на менш значущі речі, які спробує підсунути смартфон.

Варто переглянути список програм і видалити непотрібні. З корисними

додатками теж можна боротися, але для цього доведеться встановити програму. Вона дозволить задати список програм і сайтів, які потрібно блокувати на деякий час.

Смартфон створений не для того, щоб псувати зір або погіршувати розумові здібності. Це просто інструмент, і кожен сам вибирає, як його використовувати. Іноді правильний вибір – відкласти телефон і просто поспілкуватися.

(вгору)

Додаток 5

17.07.2018

Американські вчені знайшли зв'язок між зловживанням соцмережами та розладом у підлітків

Чим більше підлітки сидять у соціальних мережах і дивляться відео в Інтернеті, тим більше шансів, що у них можуть розвинутися симптоми синдрому дефіциту уваги і гіперактивності (СДУГ) (ТСН).

До такого висновку прийшли вчені з Університету Південної Каліфорнії в США, передає CNN. Свої дослідження вони опублікували в медичному журналі JAMA.

У дослідженні брали участь 2587 школярів віком 15-16 років з Каліфорнії. Протягом двох років – з 2014 по 2016 роки – школярі раз на півроку заповнювали опитувальну форму, в якій вимірювалися симптоми СДУГ.

Учасників дослідження просили згадати, скільки часу на день вони проводять, відповідаючи на повідомлення, перевіряючи соціальні мережі, здійснюючи онлайн-покупки, дивлячись відео і завантажуючи музику – усього досліджуваних активностей в Інтернеті було 14. На підставі інтерв'ю з учасниками експерименту вчені також визначали наявність та тяжкість симптомів СДУГ, які у у них проявляються: на момент початку дослідження вони не були виявлені ні в кого з підлітків.

У підсумку вчені з'ясували, що серед тих, хто користувався Інтернетом рідко, симптоми СДУГ проявлялися в 4,6% випадків. Серед тих, хто повідомляв про часте використання соцмереж (всі 14 різних активностей щодня) – в середньому 10,5 %.

Вчені кажуть, що, незважаючи на те, що взаємозв'язок між використанням соціальних мереж і проявом симптомів СДУГ був значущим, говорити про причинно-наслідковий зв'язок між ними поки що не можна. Для його підтвердження треба далі проводити дослідження.

«Якщо ми зможемо визначити, чи існує потенційний причинно-наслідковий зв'язок, тоді ми зможемо розробити заходи з припинення впливу засобів масової інформації», – сказав керівник дослідження Адам Левенталь.

Симптоми СДУГ включають в себе неуважність, гіперактивність, занепокоєння або імпульсивність, які є більш серйозними, частими або виснажливими, ніж зазвичай. За даними Центру США з контролю та

профілактики захворювань, розлад, який частіше зустрічається у хлопчиків, ніж у дівчаток, зачіпає близько 5 % всіх дітей у Сполучених Штатах. Поширеність СДУГ також оцінюється у 5 % в усьому світі.

(вгору)

Додаток 6

9.07.2018
Ирина Фоменко
Фейсбук проигрывает войну фейковым профилям

У певца Кипа Мура (Beer Money и Hey Pretty Girl) в последнее время отношения с поклонниками не заладились, пишет CNBC. На одном из концертов к нему подходили женщины с вопросом, почему он прекратил общаться с ними на Instagram или Facebook. А некоторые даже ушли от мужей после его публикации в социальных сетях о любви к фанатам (InternetUA).

«Они показывают мне документы о разводе. Говорят, что теперь мы можем быть вместе. Если я сейчас проверю почту, то там будут сотни таких сообщений. Поэтому я и не хочу в нее заходить», – поделился Мур.

Мур стал жертвой широко распространенного явления: кражи личных данных в социальных сетях. Более 28 профилей в Facebook якобы принадлежат певцу, а в Instagram – не менее 61. Мошенники пишут поклонникам, прося у них денег взаймы.

На сегодняшний день вопрос о фейковых профилях в социальных сетях стоит довольно остро. В Facebook, Instagram и Twitter очень много людей выдают себя за других, например, актеров, певцов, политиков и других известных деятелей для обмана обычных пользователей. В прошлом году австралийские власти обвинили 42-летнего мужчину в 900 детских преступлениях – он выдавал себя за Джастина Бибера на Facebook и других сайтах, чтобы просить обнаженные фотографии у несовершеннолетних.

Самозванцы бросают вызов даже самым богатым знаменитостям. В прошлом году Опра Уинфри предупредила своих подписчиков в Twitter, что «кто-то там пытается обмануть вас и выпросить деньги, используя мое имя и мой аватар в социальных сетях».

Даже топ-менеджеры Facebook, в том числе Марк Цукерберг, боролись с фейковыми профилями. Согласно исследованию Social Impostor, в Facebook, Instagram и Twitter около 9 000 поддельных аккаунтов, где люди выдают себя за 10 самых популярных людей, включая Бейонсе и Тейлор Свифт. У бразильского футболиста Неймар больше всего фейковых страниц – 1676, у Селены Гомес – 1389, у Бейонсе – 714, а у Тейлор Свифт – 233.

Твиттер, Instagram и Facebook усугубили проблему, не соблюдая собственную политику компании, запрещающую поддельные аккаунты. Facebook и Instagram взламывают фейковые профили. Как сообщили в Facebook, недавно компания внедрила программное обеспечение, автоматически обнаруживающее мошенников.

Тем не менее, в апреле количество поддельных аккаунтов возросло на 20 млн – до 80 млн, что составляет около 4 % от всех страниц в социальной сети. По словам представителей компании, проблему сложнее исправить из-за большого размера сайта.

Создание фейковых профилей

Журналист The New York Times Джек Никас провел эксперимент в социальных сетях, создавая фейковые профили. По его словам, это оказалось довольно просто.

Так, было создано восемь учетных записей на Facebook за один час на прошлой неделе. У всех аккаунтов было имя Джека Никаса, его фотография и место работы. Все, что требовалось, – это разные почтовые ящики для каждой учетной записи.

На пятом профиле Facebook заблокировал Джека из-за имени. Однако, как только он добавил средний инициал, профиль подтвердили. После создания восьми фейковых аккаунтов Facebook начал требовать номер телефона. Джек подождал несколько дней, а затем создал еще три профиля.

Фейковые учетные записи существовали на протяжении 5 дней, прежде чем Джек сообщил о них Facebook. Компания удалила их всего через несколько минут.

Джек использовал ту же почту для создания поддельных аккаунтов в Instagram, что оказалось несколько сложнее – социальная сеть запрашивала номер телефона. Но, используя несколько разных устройств, например, телефон жены, он создал 10 профилей со своим именем, биографией и фото.

Затем Никас сообщил Instagram о фейковых профилях. Социальная сеть удалила 5 профилей на следующий день. Еще четыре были активны спустя 4 дня.

С Twitter ситуация обстояла несколько лучше. После успешного создания первого фейкового аккаунта компания заблокировала фото Джека для второго профиля.

Многие сайты продают поддельные учетные записи Facebook, Instagram и Twitter. Выбор большой – есть профили с прикрепленным номером телефона или уникальными фото. Цена за учетную запись варьируется в зависимости от даты ее создания – от 5 до 40 долларов. Купить страницу можно даже за криптовалюту.

«Удручающая ситуация»

У многих знаменитостей фейковые профили могут вызвать настоящую головную боль. Американский певец Трейси Эдкинс рассказал, что фанаты после каждого его концерта спрашивали о якобы обещанных им бесплатных билетах и закулисном туре.

Когда журналист The New York Times Джек Никас написал сообщение в Instagram Эдкинсу, самозванец отправил его к профилю дочери певца. Она якобы занимается благотворительностью. Отправила фото Джеку человека на больничной койке и предложила помочь с лечением – на это нужно 14700 долларов.

Эдкинс и его команда связались с ФБР и социальными медиа, но это оказалось безрезультатно. «Они знают о фейковых профилях, но ничего с этим не делают», – прокомментировал Эдкинс.

В прошлом году певец опубликовал предупреждающее видео о поддельных учетных записях. На прошлой неделе 20 других звезд страны, в том числе Келли Кларксон и Блейк Шелтон, выпустили ролик, в котором призвали поклонников избегать фейковых профилей.

Джеймс Мартин, священник-иезуит с 571 000 подписчиков на Facebook заявил, что поддельные аккаунты просят пожертвования или «публикуют ужасные вещи от его имени».

Комик Дэйв Шапелл наблюдал за публикациями в Twitter одного из пользователей, выдающих себя за Дэйва, и даже находил его забавным – до тех пор, пока его не начал оскорблять другой комик, Кэтт Уильямс. Как позже оказалось, ни у одного из них не было своей страницы в социальной сети.

Гонка вооружений

Главная защита социальных сетей от поддельных аккаунтов – пользователи, сообщающие о подозрительной деятельности. Недавно Facebook добавил возможность сообщать о мошеннических профилях.

В ходе эксперимента Джек Никас заявил социальным сетям о всех фейковых страницах, а ответ получил только о 6 профилях в Instagram – о двух поддельных учетных записях Мура и поддельной странице Уинфри. В Instagram утверждают, что эти профили не нарушают политику компании.

«Мы серьезно относимся к сообщениям», – прокомментировал представитель Facebook и Instagram Пит Bocc. По словам представителя Twitter Яна Планкетта, у компании «строгие правила и контроль за их соблюдением».

В общей сложности Facebook удалил за январь, февраль и март примерно 583 миллиона поддельных аккаунтов, большинство сразу после создания. Программное обеспечение Twitter идентифицирует около 10 миллионов «спамных или автоматизированных» профилей в неделю.

Продуктовый менеджер Facebook Диккенс заявил, что компания пытается бороться с фейковыми учетными записями, но эта задача трудновыполнима из-за размеров социальной сети. «Это гонка вооружений», – прокомментировал Диккенс.

Война против поддельных профилей ведется в основном в Западной Африке. Большинство фейковых страниц зафиксировано в Нигерии или Гане, а их создатели – Yahoo Boys.

(вгору)

Додаток 7

10.07.2018

Французьке законодавство дозволить боротися з фейковими новинами на державному рівні

Парламент Франції ухвалив законопроект, який суттєво посилює

юридичний механізм захисту демократичного життя від фейкових новин, а також розширює можливості протидії поширенню неправдивої інформації, зокрема в передвиборний період, повідомило іноземне видання «Politiko» (Офіційний веб-сайт Національної ради України з питань телебачення і радіомовлення).

Ухвалений урядом Франції документ впроваджує нові вимоги до медіа-платформ. Для прикладу, однією з них передбачається, що такі платформи, як Facebook і Twitter, повинні зробити відкритою інформацію про джерело фінансування рекламних матеріалів.

Як раніше вже анонсувалося міністром культури Франції Франсуазою Ніссен, також цей законопроект дозволятиме блокувати фейкові новини за допомогою спеціальної судової процедури. До того ж, у випадку розміщення неправдивих повідомлень у період виборів кандидати матимуть законне право звертатися до суду з вимогою щодо їх видалення.

Найбільше голосів за ухвалення проекту закону щодо захисту від фейкових новин віддала абсолютна більшість у парламенті, яка сьогодні складається з членів центристської партії Президента Франції Еммануїла Макрона «La République en Marche.

Своєю чергою міністр культури Франції Франсуаз Ніссен також висловила велику підтримку новому закону та зауважила, що він стане цінним інструментом для кращого захисту демократії в країні. «Я в захваті від прийняття парламентом збалансованого та ефективного тексту, який піднімає це питання до значних масштабів», – наголосила вона.

Проте не всі французькі парламентарі схвально відгукнулися на адресу запроваджуваного документа. Упродовж восьми годин довкола його розгляду тривали дебати. Зокрема, одним із аргументів «проти» була заява депутата Жан-Люка Меленхона, в якій він зазначив, що цей законопроект зроблений з метою заборонити у Франції «Russia Today» і «Sputnik».

Наразі законопроект ухвалено, однак, як зазначається в повідомленні «Politiko», існує велика ймовірність, що Конституційна рада Франції може оскаржити його «у зв'язку з можливими порушеннями свободи слова».

(вгору)

Додаток 8

15.07.2018

Россию обвинили в разобщении американской нации через соцсети

Министр внутренней безопасности (МВБ) США Кирстен Нильсен заявила, что Россия пытается разобщить американцев через социальные сети. Об этом она рассказала 14 июля в Филадельфии на встрече с чиновниками, ответственными за проведение выборов в США, сообщает телеканал CNN (InternetUA).

По словам Нильсен, разведка США зафиксировала «настойчивые попытки России использовать социальные сети, высказывания сочувствующих

лиц и иные подходы, чтобы посеять разногласия и вызывать разобщенность среди американцев». Она добавила, что это не всегда связано с именами отдельных политиков или политических кампаний.

Глава МВБ считает, что пока нет свидетельств о решении России вмешиваться в промежуточные выборы 2018 года на том уровне, как это произошло в 2016 году.

«Вчерашние обвинения в отношении российских сотрудников разведки демонстрируют, что мы не потерпим вмешательства в наши демократические процессы и что иностранное вмешательство влечет за собой последствия», – прокомментировала Нильсен дело по представленным обвинениям российским военным разведчикам во вмешательство в выборы 2016 года, которые Москва опровергает.

13 июля США предъявили заочные обвинения 12 российским разведчикам по делу о вмешательстве в выборы американского президента в 2016 году. Их подозревают в проведении кибератак с целью кражи документов для их последующей публикации.

(вгору)

Додаток 9

17.07.2018
Ирина Фоменко
Как боты соцсетей могут обвалить ваши акции

Бывший политический стратег, руководитель фирмы медийной аналитики Zignal Labs Джош Гинсберг последние семь лет помогал клиентам разобраться, что о них пишут в СМИ и социальных сетях, сообщает Recode (InternetUA).

В этом году ученые Zignal начали замечать «аномалии в данных»: посты неизвестных людей, получивших признание лидеров мнений, а также всплески активности по определенным темам.

«Мы поручили нашим исследователям заняться этими данными. Оказалось, что “неизвестные люди” – боты. Огромное количество ботов оказывали влияние на корпоративные бренды и репутацию», – заявил Гинсберг.

Так, в Zignal Labs считают, что нынешние кампании дезинформации, схожие с кампаниями 2016 года, нацелены на публично торгуемые корпорации, такие как Nestlé, Harley-Davidson и AMD.

«Каждый бизнес должен осознавать этот риск. Компаниям нужно пересмотреть ведение коммуникаций, чтобы не тратить средства и время на деятельность ботов», – прокомментировал Джош. – «За последние полгода не было ни одного предприятия, которое бы не пострадало от ботов».

Гинсберг привел несколько примеров, как боты могут влиять на контент коммуникаций: от жизнеспособности корпораций до длительных культурных войн. В некоторых случаях, как и в фейковых твитах о несуществующих уязвимостях чипов AMD, боты начинают публиковать ложную информацию.

Иногда боты отвечают на реальные «проблемные» твиты – например, расистская публикация Розанны Барр о Валери Джарретт.

«Более 60 % этого диалога вели боты. Их цель – сеять вражду в медиа. Что интересно в этой ситуации, боты выступали с двух сторон – и за Розанну, и против нее. В итоге реальные люди отреагировали на этот диалог», – рассказал Гинсберг.

(вгору)

Додаток 10

18.07.2018
Ирина Фоменко
Facebook оказался замешан в фальсификации BREXIT

Избирательная комиссия Великобритании опубликовала результаты почти девятимесячного расследования по расходам на референдум Brexit и обнаружила, что официальная кампания Vote Leave нарушила закон, превысив расходы. Об этом сообщает TechCrunch (InternetUA).

Так, Vote Leave направили средства в AggregateIQ, чтобы использовать для таргетинга политическую рекламу на платформе Facebook совместно с другой кампанией Brexit BeLeave. Согласно расследованию избирательной комиссии, BeLeave потратила более 675 000 фунтов стерлингов на AggregateIQ по общей договоренности с Vote Leave.

В соответствии с законодательством Великобритании, расходы Vote Leave не должны превышать 7 млн фунтов стерлингов. Однако кампания потратила 7 449 079 фунтов стерлингов, превысив лимит почти на полмиллиона.

Facebook, сыгравший ключевую роль как основное средство коммуникаций во время референдума, заработал около 40,7 млрд долларов в 2017 году. «Без Facebook и других социальных сетей, не факт, что состоялся бы референдум, американские или итальянские выборы», – утверждает депутат Европарламента Найджел Фарадж.

Расследование избирательной комиссии было сосредоточено на финансировании и расходовании средств, и в основном касалось пяти выплат AggregateIQ в июне 2016 года тремя кампаниями (третья – Veterans for Britain). Комиссия постановила, что денежное пожертвование в размере 100 000 фунтов стерлингов, полученное и принятое 20 мая 2016 года, на самом деле было выплатой Vote Leave за услуги AggregateIQ.

Кроме того, отчет Vote Leave о пожертвованиях был неточным – еще одно преступление в соответствии с Законом о политических партиях, выборах и референдумах Великобритании 2000 года. Комиссия оштрафовала три кампании, также сославшись на члена Vote Leave Дэвида Алана Хальсалла и BeLeave Даррена Граймса в Службу столичной полиции Великобритании, которая имеет право возбуждать уголовное расследование.

В Vote Leave заявили, что доклад комиссии «содержит ряд ложных

обвинений и неверных утверждений, которые в корне ошибочны». «Удивительно, что Комиссия не допросила никого из кампании за два года», – прокомментировали в пресс-службе Vote Leave.

Facebook недавно заявил о принятии мер в отношении политической рекламы. Таким образом компания реагирует на растущее давление после скандалов, связанных с бесконтрольными публикациями. Например, на президентских выборах в 2016 году в США Facebook позволил обнародовать и распространять пророссийские посты, которые увидели сотни миллионов американских избирателей.

На прошлой неделе комиссар по информации Великобритании Элизабет Денхам раскритиковала Facebook за несоблюдение прозрачности и отсутствие контроля над сбоями, связанных с политической рекламой, а также объявила о своих намерениях оштрафовать социальную сеть за нарушение британского законодательства о защите данных (Facebook передал личную информацию 87 млн пользователей Cambridge Analytica без их ведома или согласия).

Она также опубликовала ряд политических рекомендаций в отношении цифровой политической агитации – призыв к этической паузе в отношении использования персональных данных для политического таргетинга и предупреждение об отсутствии прозрачности относительно использования личной информации пользователей.

«Без высокого уровня прозрачности – и, следовательно, доверия граждан, что их данные используются надлежащим образом – мы рискуем разработать систему наблюдения за избирателями», – заявила Денхам.

Скандал с Cambridge Analytica и Facebook связан с референдумом Brexit через AggregateIQ – компания была подрядчиком Cambridge Analytica, а также получала информацию о пользователях Facebook.

В избирательной комиссии заявили, что во время расследования к ней обратился Facebook с «некоторой информацией об использовании Aggregate IQ своих услуг во время референдума ЕС». Согласно информации Facebook, AggregateIQ использовал «идентичные целевые списки для рекламных объявлений BeLeave и Vote Leave».

«Мы также попросили предоставить копии рекламных объявлений Aggregate IQ для BeLeave и подробную информацию о полученных им отчетах от AggregateIQ. Граймс ответил на наши вопросы», – сообщается в докладе комиссии.

В разгар кампании по референдуму – в решающий момент, когда Vote Leave достигли официального лимита расходов, члены кампании убедили одного из других доноров BeLeave, Энтони Клэйка, направить пожертвования напрямую в AggregateIQ.

«11 июня 2016 года Каммингс написал Клэйку, что Vote Leave потратили почти все средства и предложил следующее: “Не могли бы вы дать 100 000 “ниндзям социальных сетей”, которые могли бы потратить их с пользой от имени этой организации? Это волне законно”. Клэйк спросил об этой организации. Каммингс ответил так: “Ниндзя социальных сетей” находятся в

Канаде. Вы отправляете деньги в их организацию, а сделка юридически будет зарегистрирована как пожертвование. С удовольствием обсужу это с вами по телефону, хотя в принципе от вас ничего не требуется, кроме как отправить средства". Затем Клэйк отправил по электронной почте Граймсу предложение о пожертвовании BeLeave. Он уточнил, что пожертвование пройдет "через счет AIQ"», – говорится в отчете избирательной комиссии.

Помимо того, что Комиссия получила доказательства «изменения AggregateIQ дизайна рекламы для BeLeave», также было установлено, что публикации Vote Leave «имели влияние благодаря внешнему виду и стратегии».

«15 июня 2016 года Граймс заявил членам Совета BeLeave и Aggregate IQ, что рекламные объявления BeLeave должны быть: "эффективным способом продвижения либеральных и прогрессивных идей для аудитории, которая, возможно, не столь восприимчива к идеям Vote Leave". 17 июня 2016 года Граймс сообщил BeLeave: "Реклама должна нормально работать с воскресенья. Я хочу убедиться, что у нас есть множество запланированных твитов и статусов для Facebook. Опубликуйте все эти блоги, используйте favstar, чтобы поделиться нашими лучшими твитами. Скопируйте и вставьте строки из брифинга Vote Leave в публикации BeLeave"», – сообщается в докладе комиссии.

В Twitter Граймс откликнулся на отчет Комиссии, спросив, почему «регуляторам» потребовалось «два года и три расследования, чтобы обнаружить неправильную регистрацию кампании 22-летнем мужчиной, который заслуживает максимального штрафа в размере 20 000 фунтов стерлингов и уголовного расследования».

Председатель комитета DCMS Дамиан Коллинз заявил, что британский избирательный закон «кажется нецелесообразным в эпоху цифровых технологий». «Следует изменить избирательный закон, чтобы он соответствовал новым технологиям. Например, чтобы все электронные кампании отвечали цифровым требованиям. В отчете "Фейковые новости" мы рассмотрим, что можно сделать, чтобы усилить полномочия таких органов, как избирательная комиссия и Управление Уполномоченного по информации», – прокомментировал Коллинз.

(вгору)

Додаток 11

5.07.2018

Майя Яровая

Комитет нацбезопасности одобрил скандальный законопроект №6688 // Эксперты: это шаг к тоталитаризму

Скандальный законопроект №6688, которым, среди прочего, предлагается блокировать сайты на 48 часов без разрешения суда, 4 июля одобрили в Комитете по вопросам национальной безопасности и обороны. Депутаты

рекомендовали Верховной Раде принять этот законопроект в первом чтении, после чего вернуть в комитет на доработку. Этот законопроект уже включили на голосование 5 июля в Раде (AIN.UA).

Мы уже рассматривали положения данного законопроекта более детально. Напомним, составители законопроекта подают его как инструмент повышения уровня кибербезопасности в стране и борьбы в информационной войне с Россией. Однако сами украинцы видят его совсем иначе.

«На самом деле это:

1. Жесточайшая цензура интернета. Хуже, чем в РФ. Блокировка ресурсов (без суда), которую вы, скорее всего, не сможете обойти. За вас будут решать, что вам показывать, а что нет.

2. Полная потеря вами анонимности. Вы не сможете пользоваться TOR, да.

3. Распил государственного бюджета на покупке оборудования и услуг от известной израильской компании Allot.

4. Детальный мониторинг вашего трафика. О вас будут знать все.

5. Снижение скорости (либо в результате мероприятий по контролю и мониторингу трафика, либо в результате ваших действий по обходу всего этого добра), и значительное повышение цен на интернет.

6. Произойдет монополизация рынка интернет-провайдеров.

Насколько все это повысит кибербезопасность нашей страны? В макроотношении – на ноль. Зеро. Ни на сколько», — пишет cybersecurity lead в компании DATAS Technology Егор Папышев.

Как отмечает директор NetAssist Максим Тульев, который присутствовал на заседании комитета, в законопроекте все намного хуже, чем казалось изначально. «Мы с Татьяной Поповой и еще парой журналистов поймали в кулуарах замначальника СБУ Олега Фролова. И задали ему ряд неудобных вопросов. В частности, о развороте заблокированных https-доменов в нашу критическую инфраструктуру. Среди прочего он сказал, что разработчик DPI, с которым они ведут переговоры, говорит, что их система может фильтровать HTTPS-трафик, так что все будет фильтроваться. На уточняющий вопрос, не пишется ли законопроект под одного поставщика оборудования, ответил, что ну требования мы выставим, может кто еще сделает такое оборудование».

Речь, очевидно, о компании Allot, о которой упомянул Папышев. Это поставщик оборудования для фильтрации трафика. По мнению Папышева, если закон примут, авторы проекта получат доступ к сотням миллионов долларов бюджетных средств на реализацию совместных проектов с Allot.

По мнению сооснователя Berezha Security Владимира Стирана, данный законопроект – это первый шаг в сторону тоталитаризма и капитального контроля над информационным полем в стране со стороны государства. «Всегда думайте о следующем шаге, который государство попытается сделать в сторону ограничения свободы и усиления безопасности. Вчера нам запретили пацакские соцсети, сегодня пытаются сделать эти запреты гибкими и удобными (читать: уязвимыми для злоупотреблений). Что будет завтра? Блокировка VPN,

которыми массово увлеклась молодежь, или сразу запрет криптографии и шифрования устройств, дисков и сообщений?» – написал он.

У данного законопроекта, помимо СБУ и ряда чиновников, есть сторонники и со стороны общества. Ранее аргументы «за» принятие №6688 высказывала юрист-криминолог Анна Маляр. Она отметила, что в реалиях, в которых Украина находится сегодня, а именно в условиях войны с Российской Федерацией, необходимы серьезные меры безопасности и противостояния информационному оружию, которые могут отличаться от методов в мирное время. Однако Маляр подчеркнула, что №6688 нуждается в серьезных доработках во избежание злоупотреблений со стороны силовиков и заинтересованных лиц.

(вгору)

Додаток 12

9.07.2018
Ирина Фоменко
Твиттер наносит удар по ботам

С октября прошлого года Twitter вдвое больше заблокировал фейковых аккаунтов в рамках постоянной борьбы с поддельными учетными записями, в том числе ботами и интернет-троллями. Об этом сообщает The Fortune (InternetUA).

Компания продолжает обеспечивать контроль после президентских выборов в США в 2016 году, спровоцировавших скандалы, связанные с пропагандой, дезинформацией и преследованиями в социальных сетях. Усилия Twitter могут привести к снижению статистики использования сайта.

Согласно данным, полученным The Washington Post и подтвержденным Twitter, компания блокирует до 1 миллиона фейковых профилей в день, а в мае и июне заблокировала 70 миллионов аккаунтов. Существенная часть процесса автоматизирована.

Автоматизированные системы идентифицируют около 10 миллионов учетных записей в месяц. Так, социальная сеть требует добавить номера телефона в «подозрительный» аккаунт. Как заявляют в Twitter, компания блокирует создание 50000 подозрительных учетных записей в день.

Большинство экспертов уверены, что значительное количество профилей – фейковые. В The Washington Post утверждают, что «чистка» может привести к снижению идентификации пользователей Twitter во втором квартале этого года. Идентификация, демонстрирующая медленный рост и фактическое снижение числа пользователей, может негативно повлиять на акции компании.

Хотя блокировка учетных записей довольно рискованна для Twitter, для социальной сети это потенциальная выгода по улучшению качества опыта взаимодействия на сайте. Twitter до сих пор не удается заблокировать фейковые профили, которые занимаются мошенничеством через криптовалюту. Именно поэтому Crypto Twitter стал менее привлекательным для пользователей.

Twitter теперь должен сосредоточиться на результатах своих главных клиентов – рекламодателей, генерирующих примерно 85 % дохода компании. Идентификация пользователей не настолько важна покупателям рекламы, как клики и продажи. Темпы роста количества пользователей в первом квартале этого года снизились до 10 % по сравнению с 14 % в 2017. В то же время выручка выросла на 21 % в 2018.

(вгору)

Додаток 13

11.07.2018

За что вас могут забанить в Фейсбуке?

Что случилось?

В последнее время Facebook стала активно рассказывать о своем внутреннем устройстве – видимо, это ответ на критику, с которой столкнулась компания после новостей об утечке данных пользователей. Недавно администрация соцсети разъяснила, за какие публикации пользователей могут забанить (InternetUA).

И что там? Порно и насилие?

Не только. В правилах выделены полтора десятка категорий запрещенной информации. Если коротко, в фейсбуке запрещены:

– порно;

– терроризм и преступления;

– насилие;

– наркотики;

– нарушение авторских прав;

– разжигание ненависти и травля.

Компания достаточно подробно рассказала о том, что считается нарушением. Например, вас могут забанить за порнографию, если вы опубликуете «изображение действий сексуального характера и обнаженного тела взрослых людей». Сюда входит как изображение самих половых органов и полового акта, так и «фетишистский контент» с изображением сцен насилия и человеческих выделений.

Фотографии обнаженной женской груди нельзя выкладывать?

Нет, нельзя. Facebook всегда боролась с изображением обнаженной женской груди, и свою политику компания не смягчила. Но хотя бы разъяснила: в социальной сети нельзя выкладывать изображение обнаженных сосков, если оно сделано не в контексте грудного вскармливания, родов, болезней и акций протеста.

Кстати, выкладывать обнаженные ягодицы крупным планом фейсбук тоже не разрешает. Правда, есть исключение: если эти ягодицы прифотошоплены к фотографии знаменитости. К сожалению, примеров в правилах не приводится.

Венеру Милосскую тоже забанят?

Нет. Facebook делает исключения для постов и картинок, публикуемых в юмористическом ключе, а также в образовательных или научных целях. Выкладывать картины, скульптуры и другие произведения искусства с обнаженной натурой администрация соцсети прямым текстом разрешает.

А если я напишу что-нибудь про секс, но без картинок?

Смотря, что вы напишете! Компания разрешает просто упоминать состояние сексуального возбуждения или половой акт, но «откровенные фразы» с подробностями запрещены.

Что значит «насилие»? Что именно запрещено?

В Facebook запрещены пропаганда самоубийств и нанесения себе увечий, а также сексуальная эксплуатация взрослых, детей и животных (в том числе демонстрация приставаний и зоофилия).

Вы также не имеете права описывать удовольствие от страдания или унижения реальных людей или животных. Выкладывать особенно жестокие видео с умирающими или мертвыми людьми (речь идет о кадрах, на которых видно расчленение, внутренние органы, обгоревшие люди или жертвы каннибализма) тоже нельзя. Фотографии с такими сценами публиковать можно, но соцсеть покажет их только совершеннолетним пользователям.

«Терроризм и преступления» – это как? Просто нельзя быть террористом?

В первую очередь, конечно, именно это: Facebook запрещает вести страницы террористическим и преступным организациям, а также массовым и серийным убийцам. Но это не все: в соцсети нельзя восхвалять такие организации и их действия, а также выкладывать их символику вне нейтрального или осуждающего контекста. Если вы планируете делать что-то подобное, лучше прочитайте подробное описание запрещенных организаций.

Описывать преступления, которые вы совершили, Facebook тоже запрещает. В частности, компания просит не писать, как вы причинили физический вред людям, занимались браконьерством или организовывали бои животных. Призывать к совершению этих действий тоже нельзя; под запретом также торговля наркотиками через Facebook.

Facebook запрещает разжигание ненависти. Что это вообще значит?

Разжигание ненависти – пожалуй, самая сложная категория запрещенной на Фейсбуке информации. Facebook относит к этой категории агрессивные или высмеивающие человеческое достоинство высказывания, а также утверждения, что та или иная группа людей неполноценна. В инструкции компании много примеров:

– нельзя сравнивать людей с грязью, бактериями, болезнями или фекалиями;

– нельзя сравнивать их с животными, «которые в данной культуре считаются низшими существами в интеллектуальном или физическом плане»;

– утверждать, что человек физически, умственно или морально неполноценен: «дефективный», «урод», «недоразвитый», «тупой», «идиот», «шлюха», «мошенник», «халявщик»;

– выражать презрение к людям или группам людей, например, словами «ненавижу», «не люблю» и «хуже всех»;

– высказывать к ним отвращение: «отстой», «мерзость», «гадость».

И вот такое тоже нельзя публиковать:

– правдоподобные угрозы и призывы к насилию в отношении каких-либо людей;

– издевательства и травля, в том числе утверждения о сексуальной жизни человека и унизительные описания внешности;

–высмеивание их болезней, травм или преждевременной смерти (в том числе предполагаемых).

Что, даже в шутку нельзя обзывать людей?

В шутку можно. В Facebook говорят, что все зависит от контекста. Если вы явно шутите или, к примеру, называете каким-то обидным словом себя самого, вас за это банить не будут.

Но назвать Гитлера мерзавцем я не могу, да?

Можете. Правила не защищают от «словесного выражения ненависти» людей, совершивших насильственные преступления или преступления на сексуальной почве.

Ну, ничего, буду обзываться в личке!

Нет, если на вас пожалуются, это может плохо закончиться. Правила запрещают отправлять людям сообщения с оскорблениями и пожеланиями смерти. Нельзя даже пытаться связаться с человеком, если он того не хочет.

Кто все это будет решать? Группа цензоров или робот?

И так, и так. За некоторыми нарушениями следят роботы – например, спам и публикации, пропагандирующие терроризм, они удаляют сами. Посты, нарушающие другие правила (в том числе о «разжигании ненависти»), роботы только находят – а окончательное решение выносят модераторы. Facebook говорит, что в компании работает 7500 «контент-рецензентов», знающих 40 языков. Им же поступают жалобы обычных пользователей.

Я стараюсь соблюдать все правила, а мой пост все равно удалили. В чем дело?!

Возможно, модератор ошибся – такое бывает. Раньше пользователи могли оспорить блокировку своего аккаунта, а теперь у них есть возможность подать апелляцию по конкретному посту — если в нем усмотрели обнаженную натуру, действия сексуального характера, враждебные высказывания или насилие. Facebook обещает рассматривать апелляции в течение суток; если выяснится, что модератор ошибся, пост восстановят.

(вгору)

Додаток 14

12.07.2018

В России предложили сажать пользователей за отказ удалить информацию из Сети

Депутаты-единороссы предложили наказывать россиян вплоть до года лишения свободы за «злостный отказ» опровергнуть или удалить из Сети «незаконную информацию», то есть данные, признанные судом порочащими честь и достоинство, экстремистскими или вредными для детей (InternetUA).

Лишать свободы предлагается тех, кто перед этим уже дважды за год был оштрафован за отказ от исполнения соответствующих решений суда.

Согласно законопроекту, который подготовили депутаты Александр Грибов, Сергей Боярский и Дмитрий Вяткин, если человек в отведенное приставами время не удалит «незаконную» публикацию, его оштрафуют на сумму от пяти до 20 тысяч рублей. В случае повторного нарушения его ждет штраф до 25 тысяч рублей или административный арест на срок до десяти суток. Для тех, кто не удалит информацию и после этого, депутаты хотят ввести уголовную ответственность – штраф до 50 тысяч рублей или лишение свободы сроком до года. Юридические лица предлагается штрафовать на сумму от 50 до 200 тысяч рублей.

Сейчас за неисполнение судебных решений гражданам грозит штраф до 2,5 тысячи рублей, а юридическим лицам – от 30 до 70 тысяч рублей. Авторы поправок в УК РФ и КоАП считают такие санкции недостаточными для нарушителей по делам «о порочащей или недостоверной информации». В комитете Госдумы по госстроительству и законодательству намерены такие поправки поддержать, сообщают «Известия».

Эксперты называют такую депутатскую инициативу спорной, ведь бороться надо с неисполнением судебных решений в целом, а не с отдельными направлениям. К тому же переводить подобные правонарушения в уголовную плоскость нецелесообразно. Вместо нового уголовного состава лучше предусмотреть механизмы и рычаги, которые обеспечат надлежащее и оперативное исполнение судебного акта.

Частично решить эту задачу помогает закон, принятый в апреле 2018 года. Если человек добровольно не удаляет данные, порочащие деловую репутацию, судебный пристав может вынести постановление об ограничении доступа к этой информации через обращение в Роскомнадзор. Этот механизм можно применить в отношении любых данных, распространение которых судом запрещено.

Кроме того, с 1 января 2016 года вступил в силу закон о праве на забвение, согласно которому теперь любой гражданин может обратиться в поисковую систему, работающую на территории РФ, с просьбой убрать не устраивающие его ссылки на сведения о нем. Поисковик, рассмотрев заявление, может принять решение либо об удалении этих ссылок, либо об отказе. В этом случае гражданин сможет обратиться в суд с требованием о прекращении выдачи ссылок на соответствующую информацию, приложив к иску официальный отказ поисковика.

(вгору)

Додаток 15

11.07.2018

СБУ запобігла кібератаці на об’єкт критичної інфраструктури

Співробітники СБ України блокували спробу російських спецслужб провести кібератаку на мережеве обладнання товариства «Аульська хлороперевливна станція», яке є об’єктом критичної інфраструктури країни (InternetUA).

Фахівці спецслужби у сфері кібербезпеки встановили, що протягом декількох хвилин системи управління технологічними процесами та системи виявлення ознак аварійних ситуацій підприємства були умисно уражені комп’ютерним вірусом VPNFilter з території РФ.

Продовження кібератаки могло призвести до зриву технологічних процесів та можливої аварії.

Задум кібератаки країни-агресора полягав у блокуванні сталого функціонування саме переливної станції, яке забезпечує рідким хлором для очищення води водопровідно-каналізаційних підприємств на всій території України.

У тісній взаємодії з адміністрацією товариства вдалося попередити потенційну техногенну катастрофу. Для блокування ураження комп’ютерним вірусом інших складових інформаційно-телекомунікаційних систем об’єкту критичної інфраструктури, недопущення можливих катастрофічних наслідків, фахівцями СБУ у взаємодії із працівниками провайдера та «Аульської хлороперевливної станції» шкідливе програмне забезпечення VPNFilter було локалізоване та знешкоджене.

У травні поточного року фахівцями СБУ вже фіксувались прояви підготовки російських спецслужб до проведення кібератаки на об’єкти державного та приватного секторів з використанням саме комп’ютерного вірусу VPNFilter.

VPNFilter – багаторівневе модульне шкідливе програмне забезпечення з універсальними можливостями, які забезпечують проведення як кіберрозвідки, так і деструктивних кібероперацій.

Завдяки поетапному розгортанню роботи Ситуаційного центру забезпечення кібербезпеки СБУ гарантує сталий ефективний захист об’єктів критичної інфраструктури держави.

(вгору)

Додаток 16

5.07.2018

Слежка за пользователями смартфонов ведется не совсем так, как мы думали

Давно существует мнение, что наши смартфоны записывают все, что происходит вокруг них и передают третьим лицам, которые смогут использовать полученные данные для таргетированной рекламы (Украинский

телекоммуникационный портал).

Исследователи из Северо-восточного университета пытались найти доказательства этого, но не нашли. Тем не менее, они нашли нечто не менее печальное.

Согласно сообщению Gizmodo, команда исследователей обнаружила, что некоторые приложения для смартфонов тайно записывают происходящее на экране устройства и передают эту информацию.

Случалось ли вам наблюдать, что стоит вам поговорить о чем-то, как вы можете увидеть рекламу этого в интернете?

Многие такое наблюдали, и объяснить это можно только тем, что компании собирают аудиозаписи, которые тайно делают смартфоны.

Для того, чтобы доказать или опровергнуть это, команда исследователей с помощью специального ПО протестировала 17260 самых популярных мобильных приложений.

В рамках тестирования изучался контент, который мобильные приложения отправляют на сервер. Ни одно из проверенных приложений не включало микрофон смартфона и не отправляла куда-либо записи с него.

Вместо этого некоторые приложения записывали происходящее на экране и отправляли эту информацию.

Некоторые приложения отправляли данные в аналитические компании. Это популярно среди разработчиков.

Так они лучше понимают пользователей. Однако, не у всех разработчиков в политике конфиденциальности указана информация об отправке скриншотов и записей экрана.

Что касается основной цели исследования, есть ограничения в тесте, которые не позволяют утверждать, что телефон совершенно точно не записывает все, что вы говорите.

Просто на данный момент не удалось найти доказательств. Наши персональные данные представляют большую ценность. Google нам это показала.

(вгору)

Додаток 17

5.07.2018

Михаил Сапитон

«Яндекс» проиндексировал Google Docs, доступные по ссылке. Как защитить информацию

Ночью с 4 на 5 июля «Яндекс» начал показывать в результатах поиска документы из сервиса Google Docs, доступ к которым распространялся по ссылке. Такие файлы может редактировать, просматривать или комментировать любой человек, получивший нужный URL – что в случае попадания в поиск означало общедоступность сведений (AIN.UA).

Лазейку закрыли спустя несколько часов. Пресс-секретарь «Яндекса» в

комментарии изданию TJournal сообщил, что компания ничего не нарушила – страницы, индексация которых запрещена в файле robots.txt, поисковик бы не стал трогать. Он также рассказал, что представители «Яндекса» уже связались с Google для оперативного решения проблемы.

Яндекс внезапно начал индексировать на http://google.docs файлы с открытым доступом. Дыру уже закрыли, но самые прозорливые успели сохранить себе номера губернаторов, таблицы со списками ночных бабочек и таблицы с прайсами популярных блогеров.

Тем не менее, пользователи сполна успели воспользоваться возможностью. Оказалось, что в Google Docs часто хранят пароли, платежные данные – в документах, попавших на первую страницу поиска, было до 80 участников. Кроме того, люди находили закрыли закрытую корпоративную информацию: не анонсированную продукцию, новые линейки или презентации для руководства. На обозрении оказались базы номеров, подборки блогеров со стоимостью размещения и другая личная информация.

При этом, искать по Google Docs можно не только в «Яндексе», но и в других сайтах, если задать фильтр с адресом сервиса. Но выдача «Яндекса» оказалась наиболее богатой по количеству слитой информации.

Как уберечь данные

Если вы беспокоитесь о каких-то конкретных документах, достаточно зайти в настройки доступа и выбрать что-то кроме «Доступно всем по ссылке». Документами можно делиться по адресу почты, например.

Если хотите убрать из публичного доступа все созданные документы, зайдите в Google Drive и следуйте инструкции:

1. Вбейте в поисковую строку type:document owner:адрес_Gmail. Замените «адрес_Gmail» на свою почту.

2. Пролистайте страницу вниз и дождитесь, пока загрузятся все документы. Затем нажмите CTRL + A (для Windows) или Command + A (для Mac). Так вы выберете все документы.

3. Кликните правой кнопкой мыши, выберите пункт «Совместный доступ» – «Расширенные». Сервис покажет список общедоступных ссылок и предложит изменить права доступа. Выберите «Доступно для выбранных пользователей» и Google Docs покажет список людей, которые могут просматривать или редактироваться документы.

(вгору)

Додаток 18

10.07.2018
Ирина Фоменко
Интернет вещей не подходит для шпионов

Безобидный обмен данными может привести к плачевным последствиям. Популярное фитнес-приложение и трекер физической активности Polar Flow определило месторасположение военного и государственного персонала,

работающего на секретных объектах. Об этом сообщает Gizmodo (InternetUA).

Согласно докладу De Correspondent и Bellingcat, через Polar Flow можно найти информацию о тренировках и использовать ее для идентификации сотрудников, работающих на военных базах и в правительственных зданиях.

Технология включала доступ к API разработчика Polar. Через API можно не только изучить общедоступные данные, но и получить приватную информацию. API также не ограничивал количество запросов, поэтому возможно, что кто-то мог собрать данные о миллионах пользователей.

Используя этот фактически беспрепятственный доступ, стало возможным идентифицировать людей, работающих на таких секретных объектах, как военные базы. По информации De Correspondent, достаточно найти государственное или военное сооружение, затем поискать данные о тренировках в этой локации, а потом изучить другие тренировки пользователя. Скорее всего, человек тренировался в своем доме или рядом с ним.

Благодаря этим данным исследователи идентифицировали более 6400 пользователей, которые, как предполагается, работают на крайне важных объектах. Среди них – сотрудники Агентства национальной безопасности США, Белого дома, Секретной разведывательной службы Великобритании MI6, российского ГРУ. Эти данные также использовались для идентификации персонала на ядерных хранилищах, шахтах для запуска ракет, в тюрьмах и Гуантанамо.

В Polar признали проблему и заявили, что в ближайшее время ее решат. «Важно понимать, что Polar не обнародовал данные и не нарушал политику конфиденциальности. В настоящее время большинство пользователей Polar сохраняют настройки личных профилей и данных по умолчанию. Хотя решение об использовании принимают клиенты, мы знаем о существующей проблеме, поэтому временно приостанавливаем API Explore», – сообщили в Polar.

Это не первый случай, когда через фитнес-приложение можно получить конфиденциальную информацию о правительстве и вооруженных силах. Ранее в этом году раскритиковали Strava: карты компании, показывающие активность пользователей во всем мире, могут использоваться для идентификации военных баз.

(вгору)

Додаток 19

9.07.2018

Функция предупреждений Firefox о вирусах в загружаемых файлах работает некорректно

В Firefox предусмотрена интересная функция – браузер автоматически отмечает загрузку из интернета вирусов и другого вредоносного ПО. Несмотря на очевидную пользу, данная функция не всегда работает корректно. Как сообщают пользователи форума Reddit, иногда в уведомлениях Firefox содержится откровенная ложь (InternetUA).

Браузер не сканирует файлы на наличие вредоносов, а лишь использует базу данных со списком подозрительных доменов, предположительно содержащих вредоносное ПО. Это было бы весьма полезно, если бы не ложные срабатывания.

Некоторые пользователи сталкивались с уведомлениями от Firefox при скачивании файлов из Library Genesis – популярного сайта для бесплатного скачивания книг и других материалов. Большая часть хранящегося на сайте контента является пиратской, однако там есть и вполне легитимные материалы, находящиеся в октрытом доступе. Тем не менее, некоторые пользователи столкнулись с тем, что при скачивании любого файла из Library Genesis браузер помечает его как вредоносный, даже если он таковым не является.

Правда, с подобным поведением Firefox сталкиваются не все пользователи. Более того, в один день браузер отмечает файлы как вредоносные, а в другой – уже нет. По словам команды техподдержки браузера, список доменов обновляется каждые 30 минут, что вполне объясняет «непостоянство» Firefox при выявлении потенциальных угроз.

По словам пользователей, сканирование отмеченных браузером файлов с помощью антивирусных решений никаких вредоносов не выявило. Даже если скачанный из Library Genesis файл является нелицензионным, вовсе необязательно он должен считаться «вирусом».

Недовольство у пользователей также вызывает отсутствие опции «Сохранить файл» в диалоговом окне уведомления. Разработчики предусмотрели только две опции, позволяющие либо открыть, либо удалить потенциально опасный файл. Другими словами, пользователь должен поверить браузеру «на слово», что файл является вредоносным, без возможности сохранить его и проверить самостоятельно с помощью антивирусных решений.

(вгору)

Додаток 20

10.07.2018

«Доктор Веб»: троянец-майнер загружается вместо обновления программ

Вирусописатели применяют различные методики распространения вредоносных программ (ITnews).

Среди них особо следует отметить использование злоумышленниками стандартного механизма обновления приложений. Именно так распространялся нашумевший троянец-шифровальщик Trojan.Encoder.12544, известный под наименованиями Petya, Petya.A, ExPetya и WannaCry-2, а также бэкдор BackDoor.Dande. Сегодня мы расскажем еще об одном подобном случае, который был подробно исследован специалистами «Доктор Веб».

В нашу службу технической поддержки от одного из пользователей поступило сообщение о том, что Антивирус Dr.Web регулярно обнаруживает и удаляет на компьютере приложение для добычи криптовалют. Исследование

журнала Антивируса показало, что майнер прятался во временной папке на зараженном ПК. В то же время журнал веб-антивируса SpIDer Gate сохранил информацию о том, что приложение пыталось соединиться с IP-адресом, который соответствует сайту компании Astrum Soft – производителя ПО «Компьютерный зал» для автоматизации компьютерных клубов и интернет-кафе.

В самом приложении официально присутствует функция майнинга (добычи) криптовалют, которую пользователь может включить, когда компьютеры простаивают.

Тем не менее, дальнейшее исследование показало, что программой, беспокоившей пользователя, было не само приложение «Компьютерный зал», а скрытый майнер, добавленный в вирусные базы Dr.Web под именем Trojan.BtcMine.2869. Этот троянец автоматически скачивался с серверов компании Astrum Soft механизмом обновления программы «Компьютерный зал» и устанавливался им в систему.

Приложение «Компьютерный зал» периодически отправляет запрос на сервер своего разработчика, в котором передает версию приложения и сведения о системе. В ответ может поступить команда на загрузку или скачивание и запуск исполняемого файла, в котором должно быть реализовано обновление программы. Однако в исследованном нами образце загружаемый на компьютер файл имеет вредоносный функционал. Это вредоносное ПО завершает работу процессов svchostm.exe и svcnost.exe, сохраняет на диск троянца-майнера и для обеспечения его автоматического запуска модифицирует системный реестр Windows. Данные о кошельке, на который перечисляется добытая криптовалюта, зашиты в теле троянца. При удалении вредоносной программы пользователем механизм обновления может скачать и запустить его заново.

На 9 июля вирусные аналитики насчитали более 2700 зараженных компьютеров, на которых действует Trojan.BtcMine.2869. В исследованном специалистами «Доктор Веб» образце троянца, загружавшегося с сервера Astrum Soft, имена инфицированных ПК (воркеров) начинаются с префикса "soyuz6_", который также записан в теле троянца. На сегодняшний день таких зараженных компьютеров насчитывается 613. Троянец распространялся в период с 24 мая по 4 июля 2018 года.

Разработчик ПО Astrum Soft и правоохранительные органы были проинформированы об этом инциденте.

(вгору)

Додаток 21

11.07.2018

ICO-проекты в числе наиболее популярных целей киберпреступников

Киберпреступники продолжают активно использовать ажиотаж вокруг цифровых денег: кроме взлома криптовалютных бирж, эксплуатации

уязвимостей в смарт-контрактах и использования зловредов-майнеров, мошенники прибегают и к классическим методам социальной инженерии (Компьютерное Обозрение).

Одна из наиболее популярных целей злоумышленников – это потенциальные ICO инвесторы (Initial coin offering – первичное размещение монет). Нередки случаи, когда киберпреступникам удаётся заполучить информацию о почтовых адресах потенциальных инвесторов определённого проекта. Тогда мошенники за некоторое время до начала старта pre-ICO рассылают фальшивые письма от лица команды проекта, в которых сообщают о старте продажи токенов и указывают адреса для перевода криптовалюты.

Также киберпреступники создают поддельные страницы, имитирующие официальные сайты ICO-проектов, и распространяют ссылки на них через электронную почту, мессенджеров, социальных сетей и рекламных объявлений в крупных поисковых системах. К примеру, путём создания фишинговых страниц, имитирующих веб-сайт ICO-проекта OmaseGo, киберпреступники смогли украсть более 1,1 млн долл.

Крупнейшим по количеству привлечённых средств на сегодняшний день является ICO Telegram: слухи вокруг него спровоцировали возникновение сотни поддельных интернет-ресурсов. Более того, как выяснили эксперты «Лаборатории Касперского», адреса кошельков, на которые злоумышленники предлагали перевести средства, делались индивидуально под каждого потенциального инвестора ICO Telegram, что затрудняло отслеживание движения средств.

Ещё один популярный метод, применяемый кибермошенниками, – это предложение перевести определённую сумму в криптовалюте, чтобы получить обратно в несколько раз больше. Первую транзакцию требуют осуществить под предлогом верификации электронного кошелька. Злоумышленники, например, создавали в социальных сетях поддельные аккаунты таких известных личностей, как технологический магнат Илон Маск и основатель мессенджера Telegram Павел Дуров, и публиковали от их лица заманчивые предложения получить большую сумму.

Раздачи происходят и якобы от имени ICO-проектов: так, мошенники сделали поддельный Twitter-аккаунт, похожий на аккаунт проекта Switcheo, и разместили в нём ссылку на предложение о бесплатной раздаче цифровых монет. В результате им удалось украсть криптовалюту на сумму более 25 тысяч долларов.

Надеяться, что интерес мошенников к криптовалюте сойдет на нет, не приходится: слишком низок порог входа в «бизнес» и слишком высока прибыль. По приблизительным подсчетам экспертов «Лаборатории Касперского» на основе информации о более тысячи известных Ethereum-кошельков злоумышленников, на которые жертвы осуществляли свои переводы, за последний год киберпреступникам удалось выманить как минимум 21 000 ETH (Ethereum – популярная криптовалюта) – более 10 млн долл. по текущему курсу. И это сумма без учёта тех средств, которые

мошенники вывели со счетов жертв самостоятельно, получив доступ к их онлайн-кошелькам.

(вгору)

Додаток 22

11.07.2018
Ирина Фоменко
Предпочитаете Gmail? Тогда прочтите это

В первых числах июля появились отчеты, подтверждающие, что сторонние разработчики приложений могли читать электронные письма, принадлежащие миллионам учетных записей Gmail. Сегодня Конгресс требует от Google ответов на множество вопросов, связанных с конфиденциальностью. Об этом сообщает The Verge (InternetUA).

Комитет энергетики и торговли Конгресса США направил 10 июля письма как Apple, так и Alphabet, задав множество вопросов о конфиденциальности. Большинство из них адресованы генеральному директору Alphabet Ларри Пейджу касательно отчета The Wall Street Journal, сбора аудиозаписей и отслеживания местоположения.

Несмотря на обещание Google перестать проверять электронные сообщения пользователей для повышения эффективности целевой рекламы, компания по-прежнему разрешает третьим сторонам читать электронные письма.

«Google по-прежнему давал доступ посторонним лицам к содержимому электронных писем пользователей, включая текст сообщения, подпись и данные квитанции для персонализации контента. Это заставляет задуматься над тем, как компания выполняет собственные обещания», – сообщается в письме.

У Тима Кука республиканцы спросили о лицемерии Apple: компания обязуется обеспечить конфиденциальность, а потом позволяет приложениям от Google и Facebook появляться в App Store. «После заявлений и действий компании возникают вопросы, как защищаются данные пользователей Apple», – говорится в обращении республиканцев.

Также законодатели заинтересовались, может ли информация, которая хранится непосредственно на устройстве, быть передана Google, Apple или сторонним разработчикам, даже если пользователи отключили службы определения местоположения. Кроме того, республиканцы обеспокоены возможностью записи аудио с устройств, когда функция «Okay, Google» отключена. Комитет попросил ответить компании на все вопросы до 23 июля.

(вгору)

Додаток 23

11.07.2018
CNN рассказал о возможной связи Mail.ru со скандалом в Facebook

Российская Mail.ru Group может быть причастна к скандалу со злоупотреблением данными Facebook, передает CNN. Пока ни о каких конкретных нарушениях не сообщается. Российская Mail.ru Group попала в сферу внимания концерна Facebook в рамках расследования о злоупотреблении пользовательскими данными британской компанией Cambridge Analytica. Как сообщает 11 июля телеканал CNN, Mail.ru Group разработала сотни приложений для Facebook, часть которых остались неопубликованными. Как сообщила пресс-служба соцсети, только два приложения получили двухнедельное разрешение на сбор данных (InternetUA).

«За последние 6 месяцев мы узнали, что у Facebook было мало возможностей для контроля за сбором и использованием пользовательских данных третьими лицами. Теперь мы узнали, что крупнейшая в России технологическая компания, чьи руководители тесно связаны с Владимиром Путиным, потенциально имела сотни приложений, которые были интегрированы с Facebook и могли собирать пользовательские данные. Если это так, нам нужно определить, какая информация была передана с помощью Mail.ru и что могло быть сделано с полученными данными», – указал Марк Уорнер, представитель Демократической партии в Сенате.

До 2015 года, в некоторых случаях, когда пользователи Facebook взаимодействовали с приложениями, созданными сторонними разработчиками, разработчик не только получал данные об этом пользователе, но и о его или ее друзьях, включая имя, пол, дату рождения, местоположение , фотографии и то, что они отмечали как «понравившееся» на Facebook. В 2014 году соцсеть объявила, что меняет политику, и ограничит доступ разработчиков к данным. Представители Mail.ru Group сообщили CNN, что российская компания запустила на платформе Facebook около 20 игр.

Расследование возможных злоупотреблений продолжается

Айми Арчибонд, вице-президент Facebook по партнерским связям, заявил CNN, что интернет-гигант пока не располагает доказательствами того, что Mail.ru Group неправильно использовала данные пользователей. Вместе с этим Арчибонд заметил, что расследование продолжается, и не стал отвечать на вопрос, есть ли у Facebook возможность определить, как российская компания использовала полученные данные. Соцсеть не сообщила, сколько пользовательских данных получено Mail.ru Group или были ли получены какие-либо данные об американских гражданах.

Mail.ru Group контролируется USM Holdings – компанией, основанной Алишером Усмановым, который был включен в опубликованный в январе министерством финансов США список бизнесменов, связанных с Кремлем. Российский инвестор Юрий Мильнер был председателем Mail.ru Group, пока не ушел в отставку в 2012 году. Мильнер сказал журналу Forbes, что он был членом тогдашней инновационной комиссии президента России Дмитрия Медведева с 2009 по 2011 год.

(вгору)

Додаток 24

13.07.2018

К популярной бесплатной утилите для удаленного доступа прилагался троян

Компания ESET предупреждает о компрометации официального сайта Ammyy Admin – популярной бесплатной программы для удаленного доступа к компьютеру. 13-14 июня злоумышленники использовали сайт для распространения вредоносного ПО под видом легитимного софта (Компьютерное Обозрение).

Пользователи, скачавшие Ammyy Admin 13-14 июня, получили в комплекте с программой многоцелевой троян Win32/Kasidet. Вредоносное ПО поддерживало две функции:

– кража файлов, содержащих пароли и другие данные авторизации криптовалютных кошельков и аккаунтов;

– поиск процессов по заданным именам.

Судя по использованию сочетания fifa2018start в доменном имени управляющего сервера, злоумышленники решили использовать для маскировки вредоносной сетевой активности бренд Чемпионата мира по футболу.

В октябре 2015 года сайт ammyy.com уже использовался для распространения вредоносного ПО. Специалисты ESET связали прошлый инцидент с кибергруппой Buhtrap.

В настоящее время история повторяется. В ESET выявили общие черты атаки 2015 года и нового инцидента. В прошлом злоумышленники распространяли через ammyy.com несколько семейств вредоносных программ, меняя их почти каждый день. В 2018 году раздается один троян, однако в трех случаях используется обфускация (запутывание) кода, позволяющая избежать обнаружения. Второе сходство – идентичное имя вредоносного исполняемого файла – Ammyy_Service.exe.

Поскольку это не первый случай компрометации сайта ammyy.com, ESET рекомендует пользователям устанавливать комплексное антивирусное ПО до загрузки Ammyy Admin. К популярной бесплатной утилите для удаленного доступа прилагался троян.

Компания ESET предупреждает о компрометации официального сайта Ammyy Admin – популярной бесплатной программы для удаленного доступа к компьютеру. 13-14 июня злоумышленники использовали сайт для распространения вредоносного ПО под видом легитимного софта.

(вгору)

Додаток 25

15.07.2018

Аккаунты украинцев воруют, а затем продают в интернете

Украинцы не заморачиваются сохранностью своих интернет профилей –

злоумышленники с легкостью уводят у них личные аккаунты и даже целые онлайн-магазины у мелкого e-commerce. В зоне риска находятся как пользователи популярных соцсетей и досок объявлений, так и мелкие предприниматели, реализующие товары с помощью крупных маркетплейсов (InternetUA).

Например, с массовой кражей Instagram-профилей пользователи столкнулись еще в 2017 году. Тогда была целая волна взломов. При этом, обращение в службу поддержки, смена паролей не приносили никакого результата – вернуть аккаунт не получалось.

«После этого Instagram добавил двухфакторную аутентификацию, ввел обязательную привязку к e-mail или номеру телефона. Но прецеденты случаются до сих пор. Как уводят профили? Взламывают пароль. Но знаю о случаях, когда данные профиля собирают во время авторизации на сайтах. Также злоумышленники могут получить ваш логин и пароль, если вы пользуетесь приложением, скачанным со стороннего ресурса, а не с официальных Playmarket/AppStore. А можно просто загуглить «взломать профиль в Instagram» и вы найдете даже специальный сайт для этого», – рассказала UBR.ua руководитель SMM направления рекламного агентства DIEVO Виктория Ляльченко.

Требуют выкуп и шантажируют

Зачастую профили перехватывают, чтобы получить выкуп за возврат аккаунта. Для этого могут даже запугивать, шантажировать, публиковать в аккаунте откровенные фото и даже писать компрометирующие сообщения подписчикам.

Чтобы не делали злоумышленники, эксперты настоятельно рекомендуют не платить злоумышленникам – взломщики не вернут вам профиль, но могут потребовать сумму еще больше.

«Сперва все же стоит оповестить службу поддержки. Если злоумышленники не вышли на связь, скорее всего, они могут продать ваши пароли/явки кому-то другому. Например, в интернете есть целые базы взломанных аккаунтов», – подметила нам Виктория Ляльченко.

Не обходят стороной воры и интернет-предпринимателей. В частности, периодическим атакам подвергаются небольшие онлайн-магазины, в том числе, размещенные на крупных украинских маркетплейсах.

«В плане безопасности все по-прежнему на очень примитивном уровне и у простых пользователей, и у небольших интернет-магазинов: пароли ставятся простые, к разным площадкам привязывается один e-mail, для создания и обслуживания нанимаются начинающие фрилансеры, которые потом годами не обновляют код сайта. Таким образом, в безопасности онлайн-площадок остается много дыр. К тому же, зачастую утечка электронных адресов пользователей, зарегистрированных на таких площадках, используется для атак на них – пользователи, видя знакомые, но подделанные атакующими, адреса отправителя и стиль сообщения открывают письма не раздумывая, открывают вложения с вредоносным кодом или переходят по вредоносным ссылкам в

письме и заражают свои компьютеры», – говорит R&D-директор «ИТ-Интегратор» Владимир Кург.

Не хотят защищаться

Чтобы избежать взлома эксперты перво-наперво рекомендуют:

– Присоедините аккаунт к e-mail и номеру телефона;

– Скачивайте приложение с официальных сервисов Google Play или App Store;

– Не авторизуйтесь на подозрительных сайтах, не вводите логин и пароль во всплывающие окна.

Сегодня электронная почта является одним из главных идентификаторов человека в интернете, к которому он привязывает аккаунты в соцсетях, в сервисах интернет-банкинга и на других ресурсах. Именно поэтому не стоит пренебрегать ее защитой, говорят эксперты.

Сегодня путей для получения доступа к ящику пользователя очень много. Это и заражение компьютера вирусом, и программы, перехватывающие весь трафик (снифферы), и «выманивание» личной информации взамен на определенный бонус (фишинг). Все эти способы взломщики используют для получения данных авторизации пользователя – логина и пароля от почты, которые и открывают доступ ко всем профилям пользователя в сети.

«При взломе профиля через почту мошенник входит в систему под логином и паролем конкретного профиля. Соответственно, сервис не может обнаружить незаконную деятельность до тех пор, пока пользователь не начинает нарушать правила площадки. Понимая данную проблему, мы регулярно проводим образовательные рассылки среди покупателей и продавцов, напоминая об основных нормах безопасности в сети. Например, первое и самое главное правило – не стоит использовать один и тот же пароль на разных ресурсах. Это значительно облегчит задачу взломщикам», – рассказали нам в OLX.

Также эксперты настоятельно рекомендуют сменить почтовый сервис, если он входит в украинский санкционный список, таких как mail.ru, yandex.ua и yandex.ru. В настоящее время доступ к ним ограничен, и вы не сможете быть до конца уверены, что ваши личные данные в безопасности.

«Не забывайте, что злоумышленник может также скрываться за незнакомыми ссылками или вирусами, которые маскируются под видом реальных сайтов, на первый взгляд мало чем отличающихся от оригиналов», – предостерегают в OLX.

(вгору)

Додаток 26

18.07.2018

Студентів техвишу викрили у поширенні шкідливої програми для прихованого майнінгу криптовалют

Вірус вражав комп’ютер жертви, після чого без дозволу власника ПК,

використовував потужності процесора для віддаленого майнінгу криптовалют. Наразі обом молодикам оголошено про підозру (InternetUA).

Працівники Слобожанського управління Департаменту кіберполіції Національної поліції України викрили двох студентів коледжу, які збували шкідливе програмне забезпечення для прихованого видобутку криптовалют.

За даним фактом було розпочато кримінальне провадження за ч.2 ст.361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) КК України.

Оперативники кіберполіції встановили, що шкідливе програмне забезпечення спільники придбали на одному з хакерських форумів. Змінивши його, студенти пропонували купити це програмне забезпечення іншим зацікавленим особам.

Окрім збуту вірусу, студенти використовували його і для власних потреб. Вони розміщували на форумах та інших інтернет-ресурсах посилання на фейкове програмне забезпечення, вражене цим вірусом, та, з його допомогою, видобували криптовалюту.

Поліцейські провели санкціоновані обшуки за місцем проживання молодиків. Під час попереднього огляду їх техніки спеціалісти виявили шкідливе програмне забезпечення, яке збували зловмисники.

Поліцейські наразі встановлюють кількість вражених цим ШПЗ комп'ютерів. Виявлену техніку направлено до експертного центру для проведення комп'ютерно-технічної експертизи.

Зловмисникам оголошено про підозру. Їм загрожує до п'яти років позбавлення волі.

Якщо ви виявили на своєму ПК наступні ознаки:

– у розділі «Диспетчер задач» наявність незнайомих або підозрілих програм, які виконуються в фоновому режимі та значно навантажують процесор

– є ознаки значного навантаження комп'ютера у той час, коли ним не користуються (підвищене тепловиділення, робота вентилятору охолодження на високих обертах) варто звернутися до спеціалістів на предмет виявлення прихованого майнера. Найчастіше «прихованість» програми-майнера забезпечується шляхом імітації під легітимний процес у операційній системі. Тому, достовірно встановити його наявність може лише спеціаліст з інформаційної безпеки.

Для того, аби унеможливити такі дії зловмисників необхідно:

– не використовувати у повсякденній роботі із комп'ютером, без нагальної на те потреби, обліковий запис з правами адміністратора;

– не завантажувати та не встановлювати не ліцензійне програмне забезпечення та програмне забезпечення не визначеного походження;

– не завантажувати та не запускати виконувані файли, які надсилаються електронною поштою;

– у випадку необхідності завантаження виконуваного файлу чи документу

з веб-ресурсу – обов'язково використовувати безпечне з'єднання (адреса ресурсу має починатися з протоколу https://) та переконатися у достовірності сертифікату (як правило – протокол у посиланні повинен бути зеленого кольору);

– регулярно оновлювати антивірусне програмне забезпечення та проводити повну (глибоку) перевірку ним операційної системи.

(вгору)

Додаток 27

18.07.2018

Хакер взломал 13 iPhone высокопоставленных лиц

Компания Cisco Talos, занимающаяся проблемами компьютерной безопасности, сообщила, что ей удалось обнаружить вредоносное ПО, при помощи которого были взломаны 13 iPhone высокопоставленных лиц Индии (InternetUA).

Используя систему управления мобильными устройствами с открытым исходным кодом – MDM, хакер смог получить доступ к переписке, данным о местонахождении и другой важной информации жертв.

Атаке подверглись 13 смартфонов Apple. Точно не известно, как именно злоумышленнику удалось зарегистрировать в MDM все гаджеты. Возможно, ему понадобился физический доступ к устройствам. Не исключено, что для этого были созданы разные ситуации, в которых жертвам пришлось разрешить третьим лицам воспользоваться их iPhone.

Подключив все гаджеты к MDM, хакер запустил на них 5 приложений. Два их них были нацелены на проверку функций устройства, одно отлеживало переписку, а два оставшихся передавали другие данные, хранящиеся на iPhone, включая GPS-координаты гаджета.

Раскрытая атака примечательна тем, что вредноносному программному обеспечению удалось замаскироваться под популярные мобильные приложения, чтобы перехватывать информацию.

Для нейтрализации угрозы инженерам Cisco Talos и Apple пришлось приложить совместные усилия. Корпорация из Купертино переработала пять разных сертификатов, на которых была построена атака.

Злоумышленник использовал метод фоновой загрузки, вставляя в программы динамические библиотеки, и несанкционированно добавлял сторонние функции в легальные и авторизованные в App Store приложения.

Таким образом, он мог незаметно для владельцев iPhone собирать информацию о номере телефона, IMEI устройства, записанных контактах, местоположении, читать переписку в различных мессенджерах, включая Telegram и Whatsapp.

Полученные данные, вероятнее всего, планировалось применять для шантажа жертв. Выбранное вредноносное ПО впервые появилось в 2015 году. Согласно данным расследования, создатель программы находится в Индии. Он

протестировал продукт на нескольких смартфонах перед тем, как атаковать 13 мобильных устройств первых лиц страны.

(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.