СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(14.02–26.02)

2019 № 4

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(14.02–26.02)
№ 4

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 2019

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

15.02.2019
Майя Яровая
Украинская соцсеть Nimses представила крупное обновление. Что поменялось?

Проект Nimses объявил о масштабном обновлении своей геолокационной соцсети. Изменился не только дизайн, но и функции приложения, кроме того внутри системы появились абсолютно новые механики.
Докладніше

***

15.02.2019
В Twitter появится возможность «уточнять» свои твиты

В данный момент Twitter не позволяет редактировать свои твиты. Так что если вы написали что-нибудь глупое, неточное или вырванное из контекста, выбор невелик. Вы можете либо смириться с содержимым твита, либо полностью его удалить (IGate).

Но скоро ситуация может измениться. Несколько часов назад, выступая на мероприятии Goldman Sachs в Сан-Франциско, глава Twitter Джек Дорси поделился соображениями насчет расширения функционала соцсети. По его словам, он раздумывает над функцией, которая позволит добавлять что-то вроде уточнения или аннотации к уже опубликованным твитам.

Сегодня люди довольно часто сталкиваются с проблемами из-за того, что они писали когда-то в прошлом. При этом у них нет возможности как-то повлиять на ситуацию. Если у пользователя появится возможность прокомментировать свой старый твит, он сможет таким образом вступить в диалог с самим собой и дать аудитории понять, что его взгляды изменились.

Сейчас пользователь может дополнить свое старое сообщение, ретвитнув его с каким-либо комментарием. Но механизм, который предлагает ввести Дорси, будет действовать несколько иначе. Комментарий, вероятно, будет добавляться под сам твит, но будет отличаться от него форматированием текста. Также весьма вероятно, что рядом с комментарием будет указана дата его добавления. Дорси пока не объясняет, как в этом случае будет работать ограничение по знакам. Также неясно, можно ли будет оставлять второй и последующие комментарии к одному и тому же твиту.

***

15.02.2019
Владимир Кондрашов

Стали известны 25 самых посещаемых украинцами доменов

На заседании Комитета ИнАУ по вопросам интернет-рекламы оглашены данные исследований интернет-аудитории Украины за январь 2019 года (InternetUA).

Исследование выполняется по заказу ИнАУ компанией Factum Group Ukraine. По итогам января 2019 г. на базе медиа-панели численностью 5 тыс. человек определен список популярных доменов, посещаемых украинскими пользователями.

В первой пятерке самых популярных в Украине доменов изменений за месяц не произошло. Она выглядит следующим образом:

google
youtube.com
facebook.com
ukr.net
vkontakte(vk.com)

Как и в прошлом месяце, кроме запрещенного в Украине «ВКонтакте» (на 5-ой позиции), в топ-25 по итогам декабря попали также российские yandex (8 позиция), odnoklassniki (ok.ru) (второй месяц удерживают 9 позицию) и mail.ru (закрепился на 15 позиции).

Исследование выполняется по заказу ИнАУ компанией Factum Group Ukraine.

***

14.02.2019
WhatsApp начинает следить за пользователями

Разработчики WhatsApp внедряет новый алгоритм отображения статусов – коротких пользовательских видео, которые отображаются в одноименном разделе. В скором будущем статусы будут сортироваться не в хронологическом порядке, а по релевантности, то есть «полезности» для пользователя (InternetUA).

Чтобы определить, какие статусы будут более или менее интересны конкретному человеку, приложение начнет отслеживать, с кем он активнее общается и чьи видео чаще смотрит. Таким образом будет собираться массив данных, на основе которого будет определяться порядок отображения статусов. Сейчас они выводятся по мере появления, то есть хронологически.

В WhatsApp утверждают, что информация о пользовательской активности будет храниться не на серверах компании, а на устройстве. Это важно – с учетом того, что личные данные пользователей Facebook (которому принадлежит WhatsApp) периодически попадают в чужие руки.

Статусами WhatsApp ежедневно пользуются 450 миллионов человек, поэтому массив данных об их активности может получиться весьма внушительным.

***

19.02.2019

В Skype теперь можно просматривать чат и список контактов в звонке одновременно

Microsoft активно работает над тем, чтобы новая версия Skype 8 предлагала не только новые модные функции, но и все особенности предыдущих релизов Skype, за которые кто-то любил этот сервис. В последнем обновлении инсайдерской версии Skype разработчики добавили возможность просматривать чат и список контактов одновременно внутри звонка. В релизной версии вы можете открыть в левой части окна либо один чат, либо список контактов (InternetUA).

Обновленная версия перенесла чат в правую часть, за счет чего левая панель освободилась для отображения списка контактов и ваших диалогов. Кроме того, теперь можно изменять правую часть с диалогом. Вместе с этим немного изменилось положение кнопок для открытия чата и создания скриншота, поэтому придется заново тренировать свою мышечную память.

***

19.02.2019

Instagram тестує стікери для збору пожертвувань в «історіях»

Розробники Instagram тестують нову функцію, яка дозволяє використовувати стікери в історіях для збору пожертвувань (Espreso.tv).

Скріншотом поділилася користувачка Джейн Манчун Вонг, передає The Verge.З 2015 року подібна функція доступна в Facebook. За допомогою таких кнопок користувачам Фейсбук вдалося зібрати близько мільярда доларів.

Стікери дозволять шукати некомерційні організації і додавати для них кнопку «Пожертвувати» в свою історію. Поки функція не додана офіційно, користувачі можуть ділитися посиланням на організацію в поле «Біо».

***

20.02.2019

Михаил Сапитон

Как выглядит украинская аудитория Telegram – исследование

Руководитель отдела аналитики TGStat Антон Проценко и продюсер издательского дома «Комитет» Лера Аркашова провели исследование украинской аудитории Telegram. Они изучили основные социодемографические характеристики и предпочтения пользователей. Данные, собранные на выборке из более чем 5000 анкет, актуальны на конец 2018 года.

Докладніше

***

21.02.2019

В Украине стал доступным YouTube Kids

В приложении YouTube Kids собраны развлекательные и познавательные ролики для всей семьи. Здесь можно найти мультфильмы детей, обучающие видео, дать детям послушать детские стишки и песенки, а также найти понятые малышам ответы на вопросы о науке, языках, математике или природе. Каналы и плейлисты сгруппированы по 4 категориям: «Шоу», «Музыка», «Обучение» и «Туризм». Дети также могут смотреть подборки видео от надежных партнерских каналов на разные темы: от декоративно-прикладного искусства до музыки, спорта, обучения и многого другого. Родители могут легко выбрать, к каким из этих коллекций и темам их дети получат доступ. Режим «Одобренные видео» позволяет родителям специально выбирать отдельные видео и каналы, чтобы сделать их доступными для своего ребенка в приложении. Если родители хотят выбрать, какой контент их дети могут просматривать в приложении, или наоборот – исключить определенные видео или каналы – это легко контролировать. При необходимости родители могут отключить функцию поиска роликов для своего ребенка (Marketing Media Review).

С помощью встроенного таймера родители могут контролировать время просмотра своих детей – например, ограничив сеанс до 30 минут. Приложение сообщит ребенку, когда его сеанс закончится. Приложение YouTube Kids является бесплатным за счет поддержки рекламы.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

20.02.2019

Вибори 2019: кандидатів просять верифікуватися у Facebook та Instagram

Кандидатів у президенти України закликали верифікувати свої акаунти у Facebook та Instagram (Факти).

Верифікація акаунтів у соцмережах потрібна для попередження недобросовісної агітації та створення fake-профілів, заявив міністр внутрішніх справ Арсен Аваков, передає прес-служба МВС.

Кіберполіція України вже провела консультації з офісом Facebook та проводитиме спеціальний моніторинг до кінця передвиборної кампанії.

– Ми виявлятимемо фейкові профілі у Facebook та Instagram, створені у період передвиборчої агітації, які використовують імена офіційно

зареєстрованих кандидатів у президенти України. А адміністрація соціальної мережі блокуватиме ці сторінки, – зазначив Арсен Аваков.

У соцмережах передбачено процедуру отримання позначки blue badge, яка підтверджує автентичність акаунту.

***

21.02.2019

#ДіяСловом: у Запоріжжі запустили флешмоб із закликом спілкуватись українською в побуті

У Запоріжжі 21 лютого стартував мовний марафон «Дій Словом», присвячений Міжнародному дню рідної мови (Espreso.tv).

Акцію ініціювали волонтери-викладачі та слухачі Безкоштовних курсів української мови у Запоріжжі. Організатори закликають запорожців спілкуватися в побуті українською мовою.

«Долучитися до марафону може будь-хто охочий у Запоріжжі. Як це виникало? Один зі слухачів у тій групі курсів, де я викладаю, запропонував таку річ: Давайте зробимо флешмоб на підтримку мови. Підтримаємо тих, хто вже говорить українською вільно, тих, хто тільки починає говорити, і тих, хто давно-давно вже хоче говорити українською, але ніяк не зважиться, бо боїться власних помилок чи якихось не таких поглядів», – розповіла викладач Безкоштовних курсів української мови у Запоріжжі Наталія Ігнатьєва.

Долучитися до марафону можуть усі бажаючі зі всієї України. Для цього потрібно зробити у соцмережах допис із хештегом #ДіяСловом і розповісти про власний досвід переходу на українську або викласти з цим хештегом відео декламації учасником віршу українською.

Перше зібрання учасників акції відбулося 21 лютого у Запорізькій обласній бібліотеці для юнацтва. Учасники записали відео та зробили фото для марафону. Ініціативу вже підтримали координатори Безкоштовних курсів української мови з інших міст. Акція триватиме до 14 березня.

***

25.02.2019

Зеленський почав обирати через соцмережі прем'єра, генпрокурора, голів СБУ та МЗС

Кандидат у Президенти і шоумен Володимир Зеленський ініціював конкурс на майбутнього прем'єр-міністра України, генерального прокурора, голів Служби безпеки України і Міністерства внутрішніх справ, які займуть ці посади за президентства Зеленського (Українські новини).

Про це йдеться у відеозверненні кандидата, опублікованому на сторінці «Команда Зеленського» в соцмережі Facebook.

«Кому подобається, коли президент призначає на посаду свого кума чи армійського друга? Чому так відбувається вже 28 років? Ми разом з тобою

написали програму “Україна мрії”. Зараз – наступний крок: “команда мрії”», – заявив Зеленський.

Далі на відео, з’являються два посилання – на сайт Зеленського та його сторінку в Facebook. На них шоумен пропонує глядачам перейти і запропонувати, хто, на їх думку, повинен бути прем’єр-міністром, генпрокурором, головою СБУ, міністром закордонних справ та міністром оборони.

«Зробимо це разом», – підсумував Зеленський.

***

25.02.2019

Мовне питання розколює суспільство? Учасники флешмобу #МоваНаЧасі пояснюють, чому ні

Українська в законі. У соцмережах триває флешмоб «Мова на часі». Ініціатори акції закликають сфотографуватися, тримаючи аркуш із написом «Мова на часі!», і поширити фото у соцмережі з відповідним коментарем та хештегом (Експрес).

Ініціатори акції хочуть спонукати Верховну Раду ухвалити закон «Про забезпечення функціонування української мови як державної» №5670-д, який має сприяти розвитку української в усіх сферах суспільного життя. Розгляд документа у другому читанні в парламенті заплановано на цей тиждень.

Акцію вже підтримали тисячі людей, серед них – громадські активісти, письменники, історики, політики, музиканти та культурні діячі.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

18.02.2019

Facebook уходит в ссылку

Исследования аналитической платформы Quintly показали, что 55 % постов социальной сети – ссылки (Телекритика).

Согласно исследованию аналитической платформы Quintly, в которым были проанализированы более 94000 Facebook страниц и более 105 млн постов, оказалось, что видеопосты генерируют больше вовлечения, чем посты со ссылками. Однако, бренды размещают все больше ссылок: «55 % из 105 млн проанализированных постов были ссылки на материалы. Изображения были использованы в 29 %, а видео составили 14 %». Конечно, такая ситуация понятна, ведь с помощью социальных сетей бренды хотят увеличить трафик на сайт, а не только поддерживать имидж бренда или его узнаваемость.

Если выстраивать контент в порядке наиболее высокого вовлечения пользователей, получаем следующее: 1 место – посты с видео, 2 место – посты с изображением, 3 место – посты со статусом, 4 место – посты с ссылками. На

сегодня размещение ссылок в постах – это единственный способ привлечения трафика на сайт из Facebook.

Quintly также проанализировало вовлечение по дням. В выходные общее вовлечение Страниц выше. У постов в выходные дни вовлечение выше на 13 %.

***

19.02.2019

Twitter змінює правила розміщення політичної реклами

Соціальна мережа Twitter вводить нові правила розміщення політичної реклами (Espreso.tv).

Про це повідомили в прес-службі компанії.

Повідомляється, що зміни торкнуться всіх країн-членів Євросоюзу, Індії та Австралії.

Згідно з нововведеннями, з 11 березня розміщувати політичну рекламу в соцмережі зможуть тільки перевірені рекламодавці з перерахованих країн.

Відзначається, що таким чином Twitter розширює свою політику щодо політичної реклами і прозорості.

***

20.02.2019

Ирина Фоменко

eMarketer: в 2019 интернет-реклама станет мировым лидером среди остальных медиа

В 2019 году сумма затраченных на цифровую рекламу средств превзойдет расходы на традиционную. Об этом сообщает TechCrunch (InternetUA).

Согласно докладу eMarketer, расходы на цифровую рекламу в США увеличатся в этом году на 19,1 %, до 129,3 млрд долларов, а на традиционную рекламу – на 19 %, до 109,5 млрд долларов. Это означает, что на цифровую долю припадет 54,2 % от общего объема, а на традиционную – 45,8 %.

Неудивительно, что большая часть денег на рекламу идет в Google и Facebook. Тем не менее, eMarketer утверждает, что доля Google на рынке фактически сократится с 38,2 % в прошлом году до 37,2 % в 2019, а доля Facebook незначительно вырастет – с 21,8 % до 22,1 %.

Судя по всему, Amazon останется основным лидером, так как рекламный бизнес в США должен увеличиться более чем на 50 %, что составляет 8,8 % от общих расходов.

«Платформа Amazon имеет неограниченное количество поведенческих данных покупателей для таргетинга и обеспечивает доступ к данным о покупках в режиме реального времени», – заявила директор по прогнозированию eMarketer Моника Пирт. – «Этот тип когда-то был доступен только через розничных партнеров. Но благодаря рекламным объявлениям

Amazon маркетологи получают беспрецедентный доступ к «полкам», где покупатели совершают покупки».

Ожидается, что к 2023 году на цифровые объявления придется более двух третей общих расходов на рекламу.

***

21.02.2019

Facebook змінить у березні правила для передвиборної реклами в Україні

Найбільша в світі соцмережа Facebook в середині березня посилить політику розміщення користувачами реклами, яка стосується майбутніх в Україні виборів президента 31 березня.

Докладніше

***

21.02.2019

Facebook работает над чипами для искусственного интеллекта

Facebook вслед за Google и Amazon начал разработку собственных чипов для искусственного интеллекта. Конечной целью компании является создание виртуального ассистента, достаточно «разумного» для того, чтобы поддерживать разговор с человеком на любую тему.

Докладніше

***

22.02.19

Социальная сеть Pinterest подала заявку на IPO

Социальная сеть Pinterest, специализирующаяся на публикации и хранении фотографий, подала в Комиссию по ценным бумагам и биржам (SEC) документы для проведения публичного размещения акций, сообщает The Wall Street Journal со ссылкой на источники (БизнесЦензор).

По их словам, компанию консультировали сотрудники Goldman Sachs и JPMorgan Chase. Выход на IPO ожидается в конце июня, однако сроки размещения могут измениться в зависимости от ситуации на рынке.

Ранее сообщалось, что Pinterest планирует IPO в первой половине 2019 года. По данным WSJ, стоимость компании при размещении может оцениваться в $12 млрд. Ожидается, что ее выручка по итогам 2018 года составит $700 млн.

Размещение Pinterest – далеко не единственное технологическое IPO, запланированное на текущий год. Среди компаний, планирующих в 2019 году стать публичными, – сервисы заказа такси Uber и Lyft, а также сервис краткосрочной аренды жилья Airbnb.

***

25.02.2019
Дмитрий Демченко
Viber будет брать от $4500 с владельцев чат-ботов

Мессенджер Viber с 1 апреля введет монетизацию для чат-ботов. Об этом сообщает TechCrunch (AIN.UA).

Минимальный тариф составит $4500 в месяц. Он позволит владельцам чат-ботов отправлять до 500000 сообщений. За $6500 Viber разрешит отправлять до миллиона сообщений в месяц. В команде мессенджера объясняют этот шаг стремлением повысить качество контента.

TechCrunch отмечает, что Viber рискует отпугнуть компании, которые используют или планируют использовать чат-боты в мессенджере. Издание приводит историю предпринимателя Эдмундаса Балчикониса, который руководит сервисом для путешественников Eddy Travels. Балчиконис рассказал, что его команда потратила восемь месяцев для создания чат-бота в Viber, но теперь сосредоточится на развитии продукта в Facebook и Telegram.

По данным компании-владельца мессенджера Rakuten, в Viber зарегистрировано более миллиарда пользователей. Мессенджер особенно популярен на Филиппинах, Мьянме и странах Восточной Европы. Viber – самый популярный мессенджер в Украине. По последним данным, он установлен на 96,4 % Android-устройств.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

19.02.2019
Focus: Все дело в эволюции – как смартфон влияет на наши отношения

«Не можешь выпустить смартфон из рук, даже когда проводишь время с друзьями или семьей? Как показывает исследование американских ученых, это отчасти связано с эволюцией», – пишет немецкий журнал Focus.

Докладніше

***

20.02.2019
Как социальные сети мешают работе и делают людей зависимыми

Каждую неделю в сети появляются новые тревожные исследования о чрезмерном использовании смартфонов и социальных сетей среди детей и взрослых. Так, в 2018 году британский государственный медиарегулятор Ofcom обнаружил, что 40 % взрослых и 65 % молодых людей первые 5 минут после пробуждения проводят в своих телефонах.

Докладніше

***

23.02.2019

Жертвы лайков. Почему дети боятся найти себя в Google и Instagram

Нравится ли современному ребенку, что мама выкладывает в Facebook и Instagram всю его жизнь – от снимка УЗИ до успехов в учебе? Американская журналистка Тейлор Лоренц пообщалась по этому поводу с несколькими детьми и родителями.

Докладніше

***

24.02.2019

Ирина Фоменко

Соцсети для подростков опаснее каннабиса

В новаторском исследовании психиатр и доцент Калифорнийского университета в Сан-Диего Кара Багот изучает, влияют ли социальные сети на мозг подростка так же, как каннабис. Установление связи может изменить отношение медицинских работников к Instagram, Snapchat и другим соцсетям, пишет The Star Online.

Докладніше

Маніпулятивні технології

18.02.2019

Как не попасться на фейки в соцсетях и новостях: украинцам дали важные советы

Любой читатель, слушатель и просто посетитель Сети может запросто утонуть в океане информации. Те, кто владеет СМИ, уже давно используют этот бесконечный поток фактов, новостей, изображений и видео, чтобы манипулировать «беззащитным Фомой». Поэтому так важно знать правила распознавания фейков, говорится в сообщении посольства США в Украине.

Докладніше

***

18.02.2019

Ирина Фоменко

Alibaba разработала пропагандистское приложение для правительства Китая

Пропагандистское приложение китайского правительства, которое недавно стало хитом, было разработано Alibaba.

Докладніше

***

21.02.2019

В НАТО перевірили стійкість військових до провокацій у Facebook

Дослідницька група Центру передового досвіду Стратегічних комунікацій НАТО створила низку фейкових акаунтів від імені військових. Мета – перевірити, наскільки фейкові облікові записи зможуть вплинути на реальні дії солдатів за допомогою маніпуляцій у соціальних мережах. Зокрема, у Facebook та Twitter.

Докладніше

***

22.02.2019

Д. Золотухін розповів NDI про можливості російського впливу на вибори

21 лютого заступник Міністра інформаційної політики України Дмитро Золотухін зустрівся з командою аналітиків National Democratic Institute (Міністерство інформаційної політики).

Заступник Міністра проконсультував експертів NDI стосовно можливості російського впливу на вибори та широко розповсюджених наративів кремлівської пропаганди. Д. Золотухін назвав можливі варіанти російського втручання в українські вибори: злам сайту ЦВК, повідомлення глядачам російських ЗМІ фейкових проміжних результатів виборів, масовані бот-атаки від так званої ольгинської «фабрики тролів».

«Коли настане березень, як вода з крану, поллються російські гроші для медіа. Проте, російська пропаганда постійно повторюється – нові фейки будуть створені в межах уже існуючих наративів», – пояснив заступник Міністра.

Саме тому, за словами Золотухіна, для аналізу інформаційного простору напередодні виборів хрестоматійним є проект МІП «Біла книга спеціальних інформаційних операцій проти України 2014-2018», у якому зібрані найпопулярніші наративи Кремля щодо ситуації в Україні.

Участь у зустрічі взяли аналітик і керівник групи Стефан Швед, аналітик із питань ґендеру та інклюзивності Мака Мешвеліані, аналітик інформаційного

середовища Келвін Ґарнер, старша менеджерка парламентської програми Ярина Одинак і координаторка програми для політичних партій Тетяна Карась.

Нагадаємо, 12 лютого відбулася презентація «Білої книги спеціальних інформаційних операцій проти України 2014-2018».

***

24.02.2019

Цукерберга «викликали на килим» борці з фейками та дезінформацією

Члени Міжнародного комітету із питань дезінформації й фейкових новин запросили на засідання у парламенті Канади власника Facebook Марка Цукерберга та керівників інших соцмереж.

Докладніше

***

24.02.2019

Українських виборців намагалися підкупити через соцмережі – поліція відкрила справу

Столичні правоохоронці розслідують можливий підкуп виборців через соціальні мережі. Про таке повідомляє прес-служба ГУ НП у Києві (InternetUA).

Як стало відомо, до столичних правоохоронців надійшла заява від директора ГО про те, що в соцмережі з'явився фейковий акаунт їхньої спільноти. На цій сторінці невідомі закликали українців брати участь в акції на підтримку одного із кандидатів на президентських виборах. За це пропонували 600 гривень винагороди.

Захід мали провести у парку міста Гайворон.

«У соціальній мережі з'явилася інформація щодо грошової винагороди за участь в акції на підтримку одного із кандидатів у Президенти України. Масовий захід запланований на 24 лютого у Кіровоградській області», – підтвердили в поліції.

Наразі поліцейські відкрили кримінальне провадження за ч. 2 ст. 160 (Підкуп виборця, учасника референдуму) Кримінального кодексу України. Санкція статті передбачає обмеження волі на строк до 3 років або позбавлення волі на той саме строк.

Спецслужби і технології «соціального контролю»

15.02.2019

Російські спецслужби через жителя Дніпра намагались втрутитися в українські вибори

Мешканець Дніпра співпрацював із російськими спецслужбами і публікував в інтернеті провокаційні матеріали про кандидатів у президенти (Espreso.tv).

Про це повідомляє прес-служба СБУ.

Чоловік контактував із мешканцем Ростова-на-Дону, який надсилав йому провокаційні матеріали про кандидатів у президенти України, аби змінити погляди виборців у місті. Ці матеріали мешканець Дніпра публікував у соцмережах.

Також він закликав у мережі до зміни територіальних меж країни.

Співробітники СБУ з'ясували, що росіянин також через соцмережі підшукував мешканців України, які мають травматичну або пневматичну зброю із відповідними дозволами, аби залучити їх до мітингів та масових заворушень напередодні та під час проведення президентських виборів в Україні.

Слідчі СБУ оголосили підозри у скоєнні злочинів проти основ національної безпеки ще двом мешканцям області, яких російські спецслужби залучили до заходів із підготовки до втручання у хід проведення майбутніх виборів в Україні.

***

18.02.2019

Военным РФ запретили размещать фото из Донбасса в соцсетях – ГУР

Во временно оккупированном Донбассе активизировали меры по недопущению утечки информации о преступной деятельности кадровых российских военнослужащих во время прохождения службы на командных должностях в составе соединений и частей террористов. Об этом сообщает Главное управление разведки Минобороны (InternetUA).

По данным украинской разведки, под предлогом недопущения утечки служебной информации личному составу российских оккупационных войск сообщили о требовании запрета размещать в социальных сетях фотографии, которые имеют какое-либо отношение к военной службе, сообщает «ЛІГА.net».

В ГУР отметили, что по результатам проверки «командирам» военных частей российских оккупационных войск запретили использовать на территории воинских частей и во время несения службы любые устройства

«Все обнаруженные устройства должны быть изъяты или уничтожены, а их владельцы будут направлены в так называемые органы государственной безопасности оккупантов», – уточняется в сообщении.

По информации источников LIGA.net в ОРДЛО, так называемым бюджетникам запретили пользоваться мобильной связью оператора Vodafone Ukraine.

***

25.02.2019

YouTube заборонить монетизацію каналів, де просувають контент проти щеплень

Як пише BuzzFeed News, представники компанії заявили, що такі відеоролики підпадають під політику відеохостингу, яка забороняє монетизацію відео з «небезпечним і шкідливим» контентом (Espreso.tv).

«У нас є суворі правила, що регулюють, які відеоролики ми дозволяємо показувати, а відеоматеріали, що пропагують антивакцинацію, є порушенням цих правил. Ми неухильно дотримуємося правил, і якщо ми знайдемо відео, що порушує їх, негайно застосуємо санкції і видалимо рекламу», – заявив представник YouTube.

Раніше на цьому тижні видання виявило, що, хоча на запит «безпечні вакцини» YouTube показує матеріали з офіційних джерел, проте не виключає з видачі «антинаукові матеріали».

Сім різних рекламодавців заявили, що вони не знали про те, що їх оголошення з'являються на таких відеороликах, які пропагують антивакцинацію.

На додаток до демонетизації контенту YouTube також ввів нову інформаційну панель, що стосується вакцин. Раніше інформаційні панелі з'являлися на відеозаписах, присвячених боротьбі з віспою, свинкою та кором, і містили тільки опис вакцини і посилання на її сторінку в Вікіпедії.

Тепер значно більшу кількість антивірусних відеороликів мають інформаційну панель з посиланнями на сторінку Вікіпедії, присвячену сумнівам щодо ефективності вакцин, де це питання описано Всесвітньою організацією охорони здоров'я як «одну з десяти глобальних загроз здоров'ю в 2019 році».

***

25.02.2019

СБУ блокировала очередную попытку вмешательства спецслужб РФ в избирательный процесс

Сотрудники Службы безопасности Украины блокировали в Сумской очередную попытку вмешательства российских спецслужб в избирательный процесс в Украине (InternetUA).

Об этом сообщают в пресс-центре СБУ.

Оперативники спецслужбы обнаружили в социальной сети «ВКонтакте» фейковый аккаунт «Роман Н», с использованием которого осуществлялось администрирования антиукраинской группы «Сумы – это Россия – Новороссия».

Сотрудники СБУ установили, что этот аккаунт был создан с противоправным использованием персональных и контактных данных жителя Сумщины без его ведома. Авторизация страницы осуществлялась с

использованием IP-адреса, принадлежащего ОАО «Национальные кабельные сети» (г. Москва, Российская Федерация).

***

26.02.2019

Facebook розблокував сторінку пропагандистів з Russia Today

Facebook розблокував сторінку російського медіа-проекту Russia Today (RT) In the Now. Це сталося після вказання інформації про материнську компанію-засновницю проекту (InternetUA).

Про розблокування повідомила ведуча телеканалу RT Анісса Науей, яка займається проектом In the Now. Саме відсутність інформації про засновників стала причиною блокування сторінки.

In the Now й усі сторінки медіа компанії Maffick, які належать російській пропагандистській компанії RT, вказали в розділі «Інформація» додаткові дані. Користувач тепер може дізнатися, що проект є брендом компанії Maffick, яка належить агентству Ruptly, власником якого є телеканал RT.

In the Now заблокували 18 лютого. Головний редактор RT Маргарита Симонян обурилася цим фактом, стверджуючи, що в In the Now не порушили правила соцмережі. Симонян вважала, що блокування відбулося після виходом матеріалу CNN про фінансування проекту Росією.

У Фейсбук пояснили блокування сторінки вимогою розкрити дані про материнську компанію.

Проблема захисту даних. DDOS та вірусні атаки

14.02.2019

Уязвимость в плагине для WordPress позволяет получить полный контроль над сайтом

Владельцы сайтов под управлением WordPress, использующие плагин Simple Social Buttons для поддержки функции репоста в соцсетях, должны как можно скорее установить обновление для плагина (InternetUA).

Исследователь безопасности компании WebARX Лука Шикич (Luka Šikić) обнаружил в Simple Social Buttons уязвимость, позволяющую злоумышленникам получить полный контроль над сайтом. Исследователь описал проблему как «ошибку проектирования приложения в совокупности с отсутствием проверки разрешений». По его словам, злоумышленник может зарегистрировать на сайте новую учетную запись и с помощью уязвимости модифицировать его основные настройки. Это даст атакующему возможность внедрить бэкдор, получить права администратора и захватить контроль над сайтом.

В опубликованном на YouTube видео Шикич наглядно продемонстрировал опасность уязвимости путем изменения адреса, привязанного к учетной записи администратора.

Исследователь уведомил разработчика плагина, компанию WPBrigade, о проблеме на прошлой неделе, и в пятницу, 8 февраля, было выпущено исправление. Администраторам сайтов, разрешающих зарегистрированным пользователям оставлять комментарии, рекомендуется как можно скорее обновить плагин до версии 2.0.22.

***

14.02.2019
Ирина Фоменко
Что такое кибератака «посредника» и как ее предотвратить

Атака посредника или «человек посередине» (man-in-the-middle, MitM) – когда злоумышленник перехватывает связь между двумя сторонами, либо тайно подслушивает, либо изменяет трафик, проходящий между ними. Хакеры могут использовать атаки MitM для кражи учетных данных или личной информации, шпионажа за жертвой, диверсии коммуникации или искажения данных.

Докладніше

***

14.02.2019
Современный умный дом – сплошная дыра в безопасности

Состояние безопасности в инфраструктуре умного дома – не просто плохое, а очень плохое. Ежегодно к сети подключаются миллионы новых устройств, разработчики которых попросту забыли подумать о защите.

Докладніше

***

14.02.2019
В Сеть утекли данные 15 млн пользователей популярного фотохостинга

Администрация популярного фотохостинга 500px сообщила об утечке персональных данных 14,8 млн пользователей сервиса в результате взлома, который произошел еще в июле прошлого года (InternetUA).

Как пишет The Verge, в сообщении уточняется, что специалисты обнаружили утечку только 8 февраля. В процессе изучения деталей они пришли к выводу, что кто-то взломал защиту сайта в районе 5 июля 2018 года. В результате этого взлома неизвестные хакеры получили доступ к именам пользователей, их логинам, адресам электронной почты, сведениям о дате

рождения, поле и местоположении (если они указывали эти сведения в профиле). Кроме того, в распоряжении злоумышленников оказались и пароли, но они хранились в зашифрованном виде.

По данным 500px, пока нет никаких свидетельств того, что хакеры использовали похищенную информацию для доступа к чужим учетным записям. Что же касается данных кредитных карт, то они не попали к злоумышленникам, поскольку 500px не хранит их на своих серверах.

В настоящее время компания продолжает расследование инцидента – за помощью в этом деле представители 500px обратились в полицию и независимую компанию, специализирующуюся на вопросах кибербезопасности. Также 500px рассылает затронутым пользователям уведомления об утечке их данных с рекомендацией сменить пароль.

***

15.02.2019

Взлом «ВКонтакте» оказался местью за «жадность» соцсети

Взлом «ВКонтакте» оказался местью хакеров. Об этом сами кибервзломщики заявили в сообществе БАГОСИ этой соцсети (InternetUA).

По словам злоумышленников, они пошли на этот шаг из-за невыплаченного вознаграждения, полагающегося за поиск и публикацию уязвимостей программного кода. При этом они заявили, что вред пользователям нанесен не был.

Хакеры отметили, что использовали ту же уязвимость, о которой сообщали администрации соцсети еще год назад, но не получили за работу даже «спасибо». На написание вредоносного кода потребовалось несколько часов.

14 февраля неизвестные разослали в личные сообщения пользователей «ВКонтакте» ссылку, при нажатии на которую во всех профилях и сообществах, которыми управляет пользователь, публиковалась одна и та же запись.

***

15.02.2019

Тысячи приложений для Android уличили в незаконной слежке

Вопреки усилиям, которые Google прикладывает для искоренения потенциально опасных приложений из Google Play, порядка 17 тысяч программ для Android ведут сбор информации о пользователях, даже если им запретили это делать.

Докладніше

***

17.02.2019

Евросоюз согласовал реформу авторского права в интернете

Европейские СМИ в будущем получат больше преимуществ перед крупными интернет-агрегаторами, такими как Google. Об этом говорится в соглашении по реформе авторского права, которое приняли представители Совета Европы, Еврокомиссии, а также Европарламента 13 февраля (InternetUA).

Реформа предполагает, что издания должны получать вознаграждение, если их материалы будут повторно использоваться агрегаторами или социальными сетями. Кроме того, вознаграждение получат и владельцы прав или создатели контента, если их песни или видеоролики распространяются через онлайн-порталы. Ожидается, что в первую очередь данная статья реформы затронет сервис видеохостинга YouTube.

Как заявил депутат Европарламента от немецкого Христианско-демократического союза Аксель Фосс, защита цифрового авторского права «положит конец эпохе дикого Запада в интернете».

Суть реформы заключается в модернизации авторского права в эпоху цифровых технологий. Ее обсуждают в Евросоюзе с 2016 года. Крупные компании, такие как Google и Wikipedia, высказывались против некоторых статей реформы.

Для вступления в силу решения его должны одобрить представители всех стран – членов Европейского союза и Европарламент.

***

17.02.2019

Twitter продолжает годами хранить удалённые пользователями личные сообщения

Пользователи социальной сети Twitter могут быть неприятно удивлены, узнав, что удалённые личные сообщения команда сервиса продолжает хранить годами. Об этом сообщил ресурс TechCrunch, получивший информацию от специалиста по безопасности Карана Саини (Karan Saini) (InternetUA).

Ошибка находится в уже не использующемся API, который тем не менее позволяет добраться до личных сообщений, даже если они были удалены как отправителем, так и получателем.

Twitter заверяет, что отключённые или удалённые аккаунты полностью удаляются со всей информацией в течение 30 дней. Но TechCrunch обнаружил, что это неверно для личных сообщений, которые можно восстановить и через много лет, в том числе и от удалённых учётных записей. Проверить это можно, запросив загрузку всей информации, которая хранится у Twitter на вашу учётную запись, даже если она была заблокирована.

***

18.02.2019

Новый троян использует антивирусы для кражи данных

ИБ-эксперты Cybereason Nocturnus Research обнаружили новую версию малвари Astaroth, которая использует легитимные процессы (в том числе и защитного ПО) в своих целях. Исследователи пишут, что троян использует продукты Avast и GAS Tecnologia для хищения данных и загрузки вредоносных модулей.

Докладніше

***

18.02.2019

Хакеры нашли способ обмануть даже самых бдительных пользователей

Недавно эксперты заметили новую фишинговую кампанию, которая может ввести в заблуждение даже самых бдительных пользователей.

Докладніше

***

18.02.2019

Британия обвинила Facebook в продаже личных данных пользователей

Британские парламентарии обвинили соцсеть Facebook в продаже личных данных пользователей и использовании антиконкурентных практик. Об этом сообщает РБК-Украина, ссылаясь на отчет британского правительства (InternetUA).

Отметим, что отчет был сделан комитетом парламента по цифровым технологиям, культуре, СМИ и спорту. Авторы утверждают, что Facebook хотел перехватывать настройки конфиденциальности своих пользователей, чтобы ряд разработчиков приложений могли получать доступ к их данным.

В отчете говорится о том, что ряд руководителей Facebook либо «умышленно вводили в заблуждение» законодателей в ходе расследования, либо «умышленно не информировали» политиков о предполагаемом вмешательстве России в зарубежные выборы. Также по словам парламентариев есть доказательства того, что иностранные государственные деятели оказывали влияние на ход голосования Brexit в 2016 году.

В ответ Facebook эти утверждения опроверг. Соцсеть заверила, что внесла значительные изменения в свою деловую политику и поддержала регулирование в таких областях, как конфиденциальность. Факт нарушения каких-либо законов в Великобритании компания отрицает.

***

18.02.2019

В Японии трех онлайн-пиратов посадили в тюрьму

В январе 2019 года в Японии трех создателей пиратских сайтов посадили в тюрьму на сроки от 2 до 3 лет лишения свободы (Телекритика).

Они администрировали сайт, который незаконно размещал комиксы манга. Так правительство Японии пытается бороться с несанкционированным распространением защищенного авторским правом контента, пишет torrentfreak, передает украинская антипиратская инициатива «Чистое небо».

Судебный иск против сайта был подан ещё в 2017 году и только теперь администраторы сайта были осуждены. «Такие суровые приговоры подают тревожный сигнал другим, занимающимся подобным. Мы, вместе с членами ассоциации, будем продолжать принимать решительные меры против злонамеренных актов нарушения авторских прав», – сказали в Ассоциации по авторскому праву на компьютерное программное обеспечение (ACCS).

Ещё в одной азиатской стране – Индии – правительство одобрило поправку к индийскому закону о кинематографии с той же целью: сдерживание воровства контента. Любой, кто записывает или транслирует фильмы без разрешения, будет приговорен к трем годам тюремного заключения и/или штрафу в размере $14 000. Ежегодно в Индии выпускается около 1000 фильмов, большинство крупных премьер быстро «пиратятся» на физических носителях (около $1 за копию) или бесплатно через интернет.

Статьей 176 Уголовного кодекса Украины также предполагается тюремный срок за организацию и финансирование сайтов, ворующих контент, на срок от 3 до 6 лет.

***

18.02.2019

Почти 3 млн частных разговоров шведов с медиками оказались слитыми в интернет

Личные разговоры почти 2,7 млн граждан Швеции с работниками медучреждений оказались в открытом доступе в интернете. Об этом сообщает издание Computer Sweden (InternetUA).

Отмечается, что большая часть звонков осуществлялась пациентами для уточнения деталей приема. При этом во время разговора раскрывались номера социального страхования, а также другие личные данные.

Как пишет издание, всего в сеть было выложено около 170 тысяч часов частных телефонных разговоров. Журналисты отмечают, что участниками инцидента стали клиенты компании Medicall, которая базируется в Таиланде. Власти Швеции, как и представители компании, пока не прокомментировали утечку данных.

***

19.02.2019

Антивирус Symantec Norton стал инструментом кибермошенников

Весьма распространенный и многими любимый антивирус Symantec Norton стал инструментом кибермошенничества. Об этом заявили сотрудники Департамента безопасности корпорации (InternetUA).

Преступники стали распространять потенциально опасные приложения под видом антивируса Norton, включая в составленный ими «зараженный» код настоящие фрагменты программы, написанные в JavaScript и HTML. Благодаря этим фрагментам им удалось создать видимость работы «настоящего» антивирусного приложения.

Отличить работу мошеннического софта от эксклюзивного позволяют несколько советов, сделанных специалистами софт-корпорации. Во-первых, установить запрет на «сканирование безопасности» файлов на жестком диске из различных браузеров. Во-вторых, так как любой антивирус поставляется со встроенной системой обновления, то не стоит загружать и устанавливать те приложения, которые предлагают «дополнительные», «усиленные», «новейшие» обновления антивируса и сканирования.

Будьте бдительны! Лучшее лекарство от мошенников – собственный разум!

***

19.02.2019

Компании и организации в США подверглись кибератакам из Ирана и Китая – NYT

Массированные хакерские атаки со стороны Ирана и Китая активизировались против США после обострения отношений администрации Трампа с этими странами, в результате чего пострадали десятки корпораций и правительственных агентств (InternetUA).

По оценкам экспертов по вопросам безопасности, кибернападения были спровоцированы выходом администрации президента Трампа с Иранской ядерной сделки, а также последнего торгового конфликта США с Китаем.

При этом уточняется, что иранские хакеры атаковали десятки корпораций, а также многочисленные агентства США, в том числе в период последнего правительственного «шатдауна» в стране.

Тем временем, активность злоумышленников из Китая была нацелена на кражу торговых и военных секретов американских военных подрядчиков и технологических компаний.

Среди предприятий, которые пострадали от кибератак, называются, в частности, компании Boeing, General Electric Aviation и T-Mobile. В самих компаниях отказались от комментариев, поэтому пока неясно, насколько успешными были действия злоумышленников из-за пределов США.

***

19.02.2019
Google запретит сайтам следить за пользователями

Google решил усилить защиту пользователей в режиме инкогнито, который в теории позволяет людям посещать сайты, не оставляя электронных следов.

Докладніше

***

20.02.2019
Microsoft поширить свій сервіс кібербезпеки у 12 країнах ЄС

Microsoft збирається розширити сервіс кібербезпеки Account Guard для 12 європейських країн, щоб захистити своїх клієнтів у політичному просторі від хакерських атак (Espreso.tv).

«Microsoft Corp у середу заявила, що запропонує свій сервіс кібербезпеки Account Guard для 12 нових ринків в Європі, включаючи Німеччину, Францію та Іспанію, щоб закрити прогалини в безпеці та захистити клієнтів у політичному просторі від злому», – йдеться в повідомленні.

Нещодавно Microsoft виявила хакерські зломи, які сталися у період з вересня по грудень 2018 року. Атаки були націлені на співробітників ради з міжнародних відносин Інституту Аспена та Німецького фонду Маршалла. У компанії вважають, що атаки, що торкнулися 104 облікових записів співробітників у Бельгії, Франції, Німеччини, Польщі, Румунії та Сербії, були проведені хакерською групою під назвою Strontium.

Зазначається, що крім Німеччини, Франції та Іспанії сервіс Account Guard також буде доступний у Швеції, Данії, Нідерландах, Фінляндії, Естонії, Латвії, Литві, Португалії та Словаччини.

Як зазначає видання, напередодні виборів до Європарламенту в травні німецькі чиновники намагаються зміцнити свою кібербезпеку.

***

20.02.2019
YouTube vs педофилия: скандал ElsaGate вне времени

После ролика блогера Мэтта Уотсона, где он утверждает, что видео с детьми привлекает внимание педофилов, которые свободно общаются в комментариях и обмениваются ссылками на детское порно, и к тому же эти видео монетизируются, YouTube попал в очередной скандал.

Докладніше

***

20.02.2019

У зашифрованих месенджерах продають дитяче порно – розслідування BBC

Безкоштовні шифровані додатки для обміну повідомленнями Telegram і Discord опинилися у центрі скандалу. Ці месенджери мають як відкриту, так і приховану сторону – і зловмисники користуються цим для розповсюдження заборонених матеріалів. Серед них – групи з продажу наркотиків, вкрадених фінансових даних та дитячої порнографії.

Докладніше

***

20.02.2019

Пользователи Android не могут отличить поддельные приложения от настоящих

Вредоносные приложения для Android, списывающие деньги с карт своих жертв, представляют даже меньшую опасность, чем поддельные банковские приложения. Такой вывод сделал исследователь в области кибербезопасности антивирусной компании ESET Лукас Стефанко.

Докладніше

***

20.02.2019

В популярных менеджерах паролей обнаружилась очень опасная уязвимость

Эксперты по безопасности постоянно советуют людям использовать менеджеры паролей. Но, оказывается, сами эти менеджеры могут быть весьма небезопасными.

Докладніше

***

21.02.2019

Владимир Кондрашов

Украинскому видеоблогеру грозит два года тюрьмы за продажу вирусов

Украинцу, который вел в сети YouTube-канал о вирусах и продавал вредоносное программное обеспечение для кражи паролей, может грозить до двух лет тюрьмы.

Докладніше

***

20.02.2019

Microsoft заявила об атаках российских хакеров на организации Евросоюза

Microsoft обнаружила новые хакерские атаки на европейские аналитические центры и некоммерческие организации, которые занимаются вопросами «демократии и прозрачности выборов» и «связаны с чиновниками». Об этом говорится в официальном блоге компании.

Докладніше

***

21.02.2019

Баг в WhatsApp для iOS позволяет обойти защиту Touch ID и Face ID

Система биометрической защиты мессенджера WhatsApp для iOS содержит уязвимость, которая позволяет обойти ее любому желающему и получить доступ к переписке.

Докладніше

***

21.02.2019

Зарегистрировано широкое распространение Android-вирусов через Instagram

Производитель антивирусного программного обеспечения «Доктор Веб» сообщил о распространении Android-троянцев при помощи сервиса Instagram.

Докладніше

***

22.02.2019

Скрытый файл в браузере Edge позволяет Facebook без разрешения пользователей запускать Flash-контент

Исследователь безопасности Иван Фратрик (Ivan Fratric) обнаружил в браузере Microsoft Edge скрытый файл, позволяющий Facebook обходить встроенные политики безопасности и без разрешения пользователей запускать Flash-контент (InternetUA).

«В Microsoft Windows есть файл C:\Windows\system32\edgehtmlpluginpolicy.bin, содержащий список доменов, которым разрешено обходить Flash click2play и без подтверждения пользователя загружать Flash-контент в Microsoft Edge», – сообщил Фратрик.

Исследователь выявил уязвимость в ноябре прошлого года. В то время список для Windows 10 (версия 1803) состоял из хешей sha256 пятидесяти восьми доменов. Фратрику удалось расшифровать и получить названия пятидесяти шести из них.

Microsoft частично исправила проблему с выходом февральских обновлений безопасности, оставив в текущей версии списка доменов, которым позволено обходить политики безопасности, только два домена Facebook (www.facebook.com и apps.facebook.com). Производитель также добавил поддержку HTTPS как обязательное требование для всех вносимых в список доменов с целью предотвращения атак «человек посередине».

Почему домены шифруются и почему Facebook по-прежнему в списке – вопросы, ответ на которые знает только Microsoft.

***

22.02.2019

Браузер Firefox 67 будет предупреждать о скомпрометированных паролях и взломанных сайтах

В будущих версиях функции Firefox Monitor улучшатся методы безопасности.

Докладніше

***

22.02.2019

Уязвимость WinRAR затронула полмиллиарда пользователей

Эксперты компании Checkpoint Research, работающей в сфере IT-безопасности, опубликовали отчёт о найденной уязвимости в коде архиватора WinRAR.

Докладніше

***

25.02.2019

WSJ: фитнес-трекеры тайно отправляют данные о пользователях Facebook

Шесть из 15 самых популярных фитнес-трекеров и мобильных приложений из раздела «здоровье» годами передавали данные о пользователях Facebook, даже не предупреждая об этом. Социальная сеть моментально узнавала об изменениях веса человека, его сердечном ритме или менструальном цикле, как только пользователь вводил эти данные в телефон, сообщила 22 февраля The Wall Street Journal. Сразу после выхода материала часть из упомянутых в статье приложений перестала делиться данными с корпорацией Марка Цукерберга, сообщает издание (InternetUA).

Журналисты WSJ проверили около 70 приложений из американских магазинов приложений AppStore и Google Play. Проверке подверглись приложения из различных разделов, в том числе предоставляющие финансовые или риэлторские услуги. По меньшей мере 11 из них передавали информацию о

пользователях Facebook, как только те входили в приложение либо добавляли новые данные о себе. При этом пользователь мог не привязывать свой аккаунт в приложении к социальной сети, но его данные все равно оказывались у Facebook. Общая аудитория этих приложений насчитывает десятки миллионов человек.

Как отмечает газета, после публикации ее статьи Facebook сама связалась с рядом рекламодателей и разработчиков приложений с просьбой прекратить подобную практику.

***

24.02.2019

Зараженные Android-приложения «съедают» до 10 ГБ мобильного трафика в месяц

Специалисты компании Oracle предупредили пользователей Android-устройств о новой вредоносной кампании, которая может обойтись им в кругленькую сумму в виде счетов за пользование мобильным интернетом.

Докладніше

***

26.02.2019

Facebook планировала следить за пользователями Android

Компания Facebook планировала использовать свое Android-приложение для отслеживания местоположения пользователей, а также разрешить рекламодателям отображать политическую рекламу и приглашать одиноких пользователей на сайты знакомств.

Докладніше

***

26.02.2019

Порошенко: Росія здійснила кібератаки на ЦВК

Президент Петро Порошенко каже, що Центральна виборча комісія 24 і 25 лютого зазнала DDoS-атак з боку Росії (Українська правда).

Про це він повідомив 26 лютого в Києві під час зустрічі з представниками IT-індустрії.

За його словами, Рада нацбезпеки і оборони разом зі Службою безпеки України, поліцією та «спільно з американськими партнерами» вже розробили механізми захисту ЦВК.

Інших подробиць президент не надав.

ДОДАТКИ

Додаток 1

15.02.2019

Майя Яровая

Украинская соцсеть Nimses представила крупное обновление. Что поменялось?

Проект Nimses нарушил долгое молчание и объявил о масштабном обновлении своей геолокационной соцсети. Изменился не только дизайн, но и функции приложения, кроме того внутри системы появились абсолютно новые механики, в которых пользователям снова придется мучительно разбираться, поскольку Nimses – не самая интуитивная в мире соцсеть. Редактор AIN.UA разбиралась, что это значит (AIN.UA).

После старта летом 2017 года, администрация соцсети надолго замолчала, прекратив все коммуникации. Как пояснили в Nimses, все это время команда занималась техническими доработками и проверкой ряда гипотез относительно экономики продукта. Пользователи чувствовали этот процесс на себе: соцсеть постоянно что-то тестировала, выкатывала и отменяла, и порой было невозможно разобраться в том, что происходит и по каким правилам работает Nimses – изменялись эти правила едва ли не каждый день.

Что нового

13 февраля команда впервые за полтора года выступила с официальным релизом и представила новый Nimses. Как сообщается, в нем экономика Nimses замкнулась в полный цикл.

Больше нимов = больше охвата

Базовая концепция проекта остается неизменной – с момента регистрации за каждую минуту жизни пользователю начисляется 1 ним. Но изменилось влияние баланса нимов на все, что делает пользователь. Теперь количество нимов на счету определяет охват постов пользователя.

Простыми словами, чем больше нимов – тем шире охват.

Каждый пользователь теперь видит соотношение своего баланса нимов с количеством людей, которые увидят его следующий пост.

Доминим

В Nimses появляется новая единица стоимости или, как это называют в самой соцсети – сущность – доминим. Один доминим равен одному году жизни в нимах, и купить его может каждый, у кого накопилось 683 748 нимов. Также стартует возможность покупки доминимов за фиатные деньги внутри приложения.

Зачем нужен доминим? Доминим добавляет охват записям пользователя, а также визуально выделяет тех, у кого он есть, но главная привлекательность доминима состоит в том, что это – единственный путь к владению Темплом (о том, что такое Темпл, можно прочитать в нашем предыдущем материале).

Стать Мастером Темпла

Как поясняют в проекте, Темплы – основа экономики Nimses. Каждый день в Темплах производятся миллионы нимов, ощутимая доля которых – это взносы жителей Темпла. Теперь у каждого пользователя есть возможность стать Мастером Темпла и забирать все взносы себе.

Стоимость занятия Темпла по всему миру начнется с одного доминима. Пользователь сможет оставаться Мастером до тех пор, пока никто не предложит больше доминимов за владение Темплом. В зависимости от количества жителей, одни Темплы будут намного привлекательней других, потому стоимость густонаселенных Темплов будет расти.

Сообщества

В новой версии Nimses появились Сообщества. Это примерно то же самое, что и в других соцсетях, но с оговоркой: основатели сообществ зарабатывают нимы. Ведь каждый новый подписчик – это +1 ним в день.

Номинации

Теперь в Nimses пользователи могут номинировать друг друга на получение статуса Ангела. Чтобы стать Ангелом, необходимо собрать 1033 номинации. Статус Ангела автоматические повышает видимость контента пользователя и, соответственно, его охваты.

Как подчеркивают в Nimses, сегодня начисленные за минуты жизни нимы – это только безусловный базовый доход, а для участия во всех аспектах жизнедеятельности проекта нимов нужно как можно больше. Тут у пользователей есть несколько сценариев заработка: приводить новых пользователей в систему; создавать тематические Сообщества; собирать подписчиков и становиться Ангелом; продавать товары и услуги в Nimses Goods; покупать доминимы за фиатные деньги.

Что убрали

В прошлом релизе Nimses команда тестировала так называемые инфинимы. Это была «сущность», равная одной человеческой жизни – 120 лет или 63 115 200 нимов. Чтобы купить инфиним, необходимо было также уплатить 30 % пользовательского взноса, получается чуть больше 82 млн нимов. За каждый инфиним Nimses обещала выплатить его владельцу ни много ни мало 15 000 евро.

Этим пользовались многие торговцы на площадке Goods. Нужно было всего лишь продать товара на 82 млн нимов – и забирай выторг в валюте. В октябре 2018 года в Nimses нам сообщили, что некоторые торговцы таким образом сумели конвертировать свои запасы нимов.

С исчезновением инфинима заметно изменилась экосистема Goods. Если раньше здесь можно было купить много разных товаров сугубо за нимы, то теперь многие торговцы не хотят отдавать свои товары вот так: в маркете остались преимущественно «скидки» – когда ты платишь 50 % стоимости нимами, а остальное перечисляешь реальной гривной.

(вгору)

Додаток 2

20.02.2019
Михаил Сапитон
Как выглядит украинская аудитория Telegram – исследование

Руководитель отдела аналитики TGStat Антон Проценко и продюсер издательского дома «Комитет» Лера Аркашова провели исследование украинской аудитории Telegram. Они изучили основные социодемографические характеристики и предпочтения пользователей. Данные, собранные на выборке из более чем 5000 анкет, актуальны на конец 2018 года (AIN.UA).

Журналист AIN.UA приводит основные выдержки из исследования.

Аудитория Telegram почти поровну распределена по полу (48 % женщин и 52 % мужчин). Больше всего пользуются мессенджером люди в возрасте от 18 до 24 лет. Следующая по величине возрастная группа – 25-34 года.

Больше всего в Telegram опытных наемных работников и студентов. Меньше всего – учеников и безработных.

При распределении по доходу лидирует категория пользователей без заработка. На втором месте – люди с доходом от 5000 до 10000 грн.

Почти половина пользователей Telegram, принявших участие в опросе, живут в Киеве (47,6 %) или Киевской области (49,2 %).

Как пользуются мессенджером

Android предсказуемо лидирует по популярности на мобильных устройствах – операционка установлена на смартфонах 70 % украинских Telegram-пользователей. Остальные 30 % заняла iOS.

Доля неофициальных клиентов в общей статистике пользования незначительна, но на Android такие приложения популярнее.

Распределение по настольным ОС показывает перевес в пользу Windows и веб-версии мессенджера. На третьем месте – macOS.

У большинство пользователей Telegram соседствует с другими социальными сервисами. Самое большое проникновение – у Instagram и Viber. На заблокированный «ВКонтакте» приходится всего 14 %.

Зачем пользуются мессенджером

Три четверти украинских пользователей Telegram ценят мессенджер за удобство. Среди других преимуществ: активное общение и доступ к информации.

Более половины опрошенных считают, что каналы – удобнее чем группы в Facebook. Примерно столько же отдают предпочтение групповым чатам в мессенджере.

А вот секретные чаты не очень востребованы.

В списке главных целей использования уверенно лидируют чтение каналов и личная переписка. Небольшие групповые чаты (до 50 участников) и боты тоже сравнительно популярны. При этом почти 20 % опрошенных ведут свои каналы.

Больше всего пользователей читают от 6 до 15 каналов.

Самые популярные каналы – с образовательным и новостным контентом, а также авторские блоги и подборки мемов.

Оповещения от каналов чаще всего отключают. Но треть пользователей разрешает нотификации от избранных источников.

Опрошенные в исследовании пользователи чаще всего имели от 26 до 50 зарегистрированных в Telegram контактов. Вторая по популярности группа – люди с 11-25 контактами.

Зачем проводили исследование

По словам Антона Проценко, исследование провели из-за интереса к рынку, который значительно вырос за 2018 год:

– Мы в TGStat постоянно следим за развитием экосистем каналов на разных рынках. Давно заметив на сервисе рост каналов в украинском сегменте Telegram (за 2018 год количество каналов выросло больше чем в шесть раз), мне стало интересно изучить рынок в деталях.

И если для меня это в первую очередь исследовательский интерес, то для рынка, я верю, это исследование будет очень полезно по ряду причин. Во-первых, до сих пор просто не было подробного исследования соцдема и предпочтений пользователей – а это накладывает отпечаток и на администраторов, которые не знают свою аудиторию, и на бизнес, который боится приносить администраторам деньги, потому что не хочет играть вслепую. В менее глобальном плане, исследование помогло каждому принявшему участие администратору понять, для кого пишет конкретно он – так как по итогу мы визуализировали все выкладки по каналам.

Это не первое исследование Telegram-аудитории, которое проводит Проценко. В 2017 году он уже опрашивал пользователей. При сборе новых данных, он столкнулся с высоким уровнем отказов – на размещение Google-формы с вопросами согласились не более 30 % администраторов:

– Ранее я уже проводил такие исследования с Максимом Кажданом: мы опросили чуть больше 20 000 человек в русскоязычном Telegram в 2017, и в дополнении к масштабному российскому исследованию сделали анализ украинских подписчиков русскоязычных Telegram-каналов. Тогда было тяжело проводить дополнительное исследование украиноязычных пользователей, так как украинских каналов всего было около 120.

Результатами текущего исследования мы с Лерой Аркашовой, продюсером «Комитета», довольны, но процент отказов нас расстраивал. Многие администраторы не понимали, зачем им это нужно, хотя мы описывали все детали. Многих смущало, что я из России, и меня подозревали в связях примерно со всеми структурами, какие можно представить. Процент согласившихся колебался на уровне 20-30% (аналогичный показатель в 2017 был выше в разы). Это был новый опыт, и мы особенно благодарны тем каналам, которые поддержали наше стремление сделать рынок более открытым и изученным.

(вгору)

Додаток 3

21.02.2019

Facebook змінить у березні правила для передвиборної реклами в Україні

Найбільша в світі соцмережа Facebook в середині березня посилить політику розміщення користувачами реклами, яка стосується майбутніх в Україні виборів президента 31 березня (Espreso.tv).

Про це повідомила продакт-менеджер Facebook Сара Шифф.

«З минулого тижня ми почали тимчасово забороняти зарубіжну передвиборчу рекламу щодо України. Це частина наших заходів щодо запобігання зовнішнього впливу. Крім цього, в середині березня ми маємо намір встановити (*в Україні - ред.*) нові правила розміщення політичної реклами, аналогічні тим, які раніше були встановлені в США, Бразилії, Індії та Великобританії», – сказала вона.

За словами Шифф, нові правила передбачають більш жорстку ідентифікацію осіб, які розміщують таку рекламу.

«Ми будемо вимагати від таких осіб надання дійсних документів про ідентифікацію особистості, і підтвердження, що вони є тими, ким представляються. Це одне з наших зобов'язань: забезпечити, що за політичною рекламою в Facebook стоять справжні обличчя», – сказала Шифф.

Водночас, вона повідомила, що нова політика передбачає більш широкі можливості щодо вивчення розміщеної реклами.

«Можна буде побачити більше інформації про виконавців, скільки часу було витрачено на рекламу, скільки вона зібрала емоцій, чи є вона актуальною, демографічний зріз про осіб, що переглянули рекламу: вік, стать, місце. Вся ця інформація буде розміщена в так званій "бібліотеці реклами", яка доступна для загального ознайомлення», – пояснила представник Facebook.

(вгору)

Додаток 4

21.02.2019

Facebook работает над чипами для искусственного интеллекта

Facebook вслед за Google и Amazon начал разработку собственных чипов для искусственного интеллекта. Конечной целью компании является создание виртуального ассистента, достаточно «разумного» для того, чтобы поддерживать разговор с человеком на любую тему. Об этом рассказал глава ИИ-лаборатории Facebook Ян Лекун (Yann LeCun) в интервью Financial Times (InternetUA).

Facebook также хочет расширить применение ИИ для контроля над социальной сетью. В частности, что касается мониторинга видео в режиме

реального времени и помощи модераторам при принятии решений о том, насколько допустимым является тот или иной контент.

Компания недавно запустила совместный проект с Intel, но также разрабатывает свои собственные ASIC для поддержки ИИ-программ. В Facebook начали работу в этом направлении, когда поняли, что для прорыва в области искусственного интеллекта им нужны более быстрые вычисления, чем те, что уже доступны на рынке.

Компания также работает над новым дизайном для нейросетей, которые являются сердцем систем глубинного обучения, используемых для распознавания изображений и речи. Работая в Bell Labs компании AT&T, Ян Лекун создал первую в мире конволюционную нейронную сеть. Теперь он трудится над созданием нового дизайна нейросетей для Facebook.

По словам Лекуна, Facebook делает ставку на так называемые «self-supervised» системы, которые способны делать более обширные прогнозы об окружающем их мире, а не только выводы, непосредственно связанные с теми данными, на которых они были обучены. Это нужно для того, чтобы будущий виртуальный ассистент обладал некоторым уровнем «здравого смысла» и мог поддерживать полноценный диалог.

На данный момент работа над созданием такого рода компьютеров находится в зачаточном состоянии.

(вгору)

Додаток 5

19.02.2019

Focus: Все дело в эволюции – как смартфон влияет на наши отношения

«Не можешь выпустить смартфон из рук, даже когда проводишь время с друзьями или семьей? Как показывает исследование американских ученых, это отчасти связано с эволюцией», – пишет немецкий журнал Focus (InternetUA).

Команда исследователей под руководством профессора психологии Дэвида Сбарры из Аризонского университета проанализировала имеющиеся исследования, посвященные влиянию смартфонов на коммуникацию между людьми.

Ученые установили: в том, что люди отвлекаются на свои телефоны в ущерб общению с другими людьми в реальной жизни, большую роль играет эволюция. «Люди хотят быть на связи с другими. В ходе эволюции человек тоже всегда полагался на тесные взаимоотношения со своей семьей и друзьями. Эти отношения были необходимы для выживания в качестве индивида и биологического вида. При этом эта модель основывалась на доверии, которое возникает, когда человек передает информацию и реагирует на информацию других», – поясняет автор статьи.

Сегодня такое взаимодействие облегчается смартфонами. «Тяга к смартфону связана со старыми программами в мозге, которые имели значения

для нашего выживания», – рассказал Сбарра в разговоре с изданием Science Daily.

«Смартфоны и социальные сети дают возможности для предоставления информации и реакции на других. Однако, – подчеркивает исследователь, – виртуальные связи могут воздействовать и на существующие отношения». Чтобы полностью понять положительное и отрицательное воздействие виртуального общения на реальные отношения, необходимо провести дополнительные исследования, передает Focus.

(вгору)

Додаток 6

20.02.2019

Как социальные сети мешают работе и делают людей зависимыми

Каждую неделю в сети появляются новые тревожные исследования о чрезмерном использовании смартфонов и социальных сетей среди детей и взрослых. Так, в 2018 году британский государственный медиарегулятор Ofcom обнаружил, что 40 % взрослых и 65 % молодых людей первые 5 минут после пробуждения проводят в своих телефонах. Более половины опрошенных также заявили, что их устройства мешают личным беседам с друзьями и семьей. Но как это влияет на рабочую жизнь? Вот, что выяснило международное деловое издание Financial Times (InternetUA).

Бремя рабочих писем

Бремя электронных писем, которые продолжают поступать в почтовые ящики даже после окончания рабочего дня, может оказать негативное влияние на психическое здоровье.

«Именно массовое внедрение электронной почты на мобильные устройства положило начало современной эре “технострессов”», – говорит Кэри Купер, профессор психологии в Манчестерской бизнес-школе.

Купер является сопредседателем Национального форума по вопросам здоровья и благополучия на работе, объединившего крупных работодателей (таких как British Telecom, British Petroleum и Shell) с представителями правительства, здравоохранения и социальных сетей. Их цель – снизить уровень стресса и повысить производительность работников.

Постоянная проверка смартфонов перегружает, отвлекает от работы, мешает отдыхать ночью и общаться со своими семьями.

С этим согласен Пол Макларен, психиатр из Приоратской больницы в Кенте.

«Возможность доступа к электронной почте из любого места, от туалета до вершины горы, усложняет жизнь людям, которым сложно разграничивать работу и отдых. “Затишье” на выходных и в праздничные дни сменяется потоком входящих писем, а световые или звуковые оповещения могут стать настолько неотъемлемой частью нашего сенсорного восприятия, что без них мы начинаем чувствовать дискомфорт», – говорит он.

Ричард Маккиннон, профессиональный психолог и управляющий директор WorkLifePsych, придерживается аналогичной точки зрения.

«Руководители, с которыми я работаю, называют почту одним из главных факторов стресса на работе. Их задача – формировать и реализовывать стратегию, но в восемь, девять, десять часов вечера они все еще разбирают рабочую почту, чтобы на следующий день папка “Входящие” снова заполнилась», – рассказал он.

Франция признала эту проблему, введя закон, гарантирующий работникам право «отключаться» после того, как они покинут рабочее место. На корпоративном уровне некоторые крупные немецкие компании предпринимают попытки справиться с перегрузкой. Автомобилестроительный концерн Daimler автоматически удаляет электронные письма сотрудников, когда они находятся в отпуске, а Volkswagen блокирует их в нерабочее время (доступ открывается, когда люди возвращаются на работу).

Законодательство, однако, не решит всех проблем.

«Как только вы создаете закон, люди начинают искать лазейку», – констатирует Маккинон. Строгие правила также препятствуют гибкости, которую предпочитают некоторые работники.

Вместо этого в Великобритании разработали руководящие принципы, которые помогут компаниям установить баланс между благополучием работников и преимуществами связи. К ним относятся уважение к свободному времени коллег, отказ от переписки в формате «Ответить всем» и регулярные напоминания о возможности ухода в оффлайн, например, «Пятницы без электронной почты».

Изменения должны идти сверху, говорит Дэвид Д’Суза, директор Королевского института персонала и развития.

«Руководители должны осознать, что ответ на электронное письмо в субботу вечером в 10 часов отсылает организации четкий сигнал: наиболее успешными людьми являются те, кто работает, не останавливаясь. А это может иметь серьезные последствия для здоровья», – говорит он.

Навязчивые социальные сети

«Политика многих компаний запрещает использование корпоративных устройств для личных целей в рабочее время. Но, если зависимость достаточно сильна, люди все равно будут это делать. Большинство людей переписываться в Facebook в течение рабочего дня, и грань между личным и рабочим временем размывается», – считает Макларен.

Чрезмерное использование социальных сетей пока не стало большой проблемой для работодателей. До сих пор соцсети больше беспокоили компании в контексте репутационных рисков из-за ошибочного твита или неудачного обновления статуса. Но хотя эффект социальных медиа не считается таким же вредным, как пристрастие к онлайн-казино, он уже вызывает беспокойства из-за влияния на рабочую и личную жизнь.

Психотерапевт и эксперт по зависимостям Сьюзен Хепберн из Лондона говорит, что число людей, обращающихся в связи с зависимостью от

социальных сетей, за последние 8−10 лет значительно возросло. Некоторые даже потеряли из-за этого работу.

В современных смартфонах существуют функции, позволяющие ограничивать количество времени в выбранных приложениях (например, Apple Screen Time). И хотя их разрабатывали в ответ на проблему чрезмерного использования соцсетей, Маккиннон и Д'Суза считают, что сами по себе они вряд ли ответственны за снижение производительности.

«Люди, использующие Facebook на работе, очевидно, тратят время зря. Но исторически мы всегда находили время и способ отвлечься», – говорит Д'Суза.

Хепберн, однако, считает, что, если компании не обратят на эту тенденцию достаточно внимания, однажды она сможет стать проблемой.

«Многие работодатели не применяют строгие или четкие правила в отношении использования социальных сетей на работе. Поэтому сотрудники считают, что при отсутствии серьезных последствий регулярно проверять свои страницы в соцсетях – нормально. К сожалению, это может перерасти в более серьезную зависимость», – уверена она.

Хепберн предлагает простые решения, которые должны отвлечь сотрудников от непрерывного потока информации в социальных сетях. Это могут быть организованные встречи команды, групповые обеды или занятия, такие как йога. Тем не менее, предприятиям придется принять, что границы между тем, что является и не является работой, стираются с приходом новых технологий.

Если работодатели замечают, что сотрудники чрезмерно используют социальные сети, необходимо пересмотреть организацию рабочего процесса.

«Причиной может быть скука, беспокойство, неуверенность в том, что делать дальше. Также это может быть просто чувство перегруженности работой», – говорит Маккиннон.

Бесконечный поиск социального одобрения

Работая в сфере связей с общественностью, Дженнифер Моррис признается, что слишком много времени проводит в телефоне и социальных сетях. Она не только управляет страницами в Facebook и Twitter на работе, но и ведет Instagram-канал собственной торговой марки.

«Я стараюсь быть внимательной, но это так сложно. Трудно устоять, сталкиваясь со всеми уведомлениями о новом контенте и сообщениях, – говорит Моррис. – Вас засасывает в бесконечный скроллинг, и вы можете обнаружить, что уже 45 минут сидите на кровати, ничего не делая. В некотором смысле это как наркотик».

Согласно отчету Kleiner Perkins Internet Trends, в 2018 году средний взрослый тратил на цифровые устройства по 5,9 часа в день. Согласно отчету Kleiner Perkins Internet Trends, на смартфоны приходилось по 3,3 часа. При этом в социальных сетях люди проводят по 2,3 часа в день, тогда как 5 лет назад на это уходило 1,5 часа.

Некоторые пользователи Интернета заглядывают в социальные сети значительно чаще. Так, хотя Моррис осведомлена о негативных последствиях зависимости от соцсетей, каждые несколько минут ей хочется взять телефон и проверить обновления (даже если она в это время занята на работе).

Некоторые из создателей социальных сетей критично отзывались о своих проектах. Чамат Палихапития, бывший вице-президент Facebook, в 2018 году заявил: «Мы создали инструменты, разрывающие саму социальную структуру общества. Все эти короткие сеансы обратной связи разрушают принципы того, как люди должны взаимодействовать. Лайки, репосты – это краткосрочные дофаминовые петли обратной связи. Вы эксплуатируете уязвимость человеческой психики».

Когда Моррис впервые открывает настройки iPhone, чтобы увидеть, сколько времени она тратит на социальные сети, женщина не верит своим глазам.

«32 часа и 26 минут в неделю. Как так? Это совершенно абсурдно», – говорит она.

Другой специалист по связям с общественностью Сэм Блайберг не скрывает, что у него есть проблема с зависимостью от соцсетей.

«Показательными являются рефлексивные порывы проверять социальные сети несколько раз в час, когда это действительно не нужно, – говорит он. – Я осознал эту проблему, когда заметил, что не могу не проверять свой телефон во время просмотра фильма с семьей. Точно так же я чувствую, что больше не могу читать книгу, не проверяя уведомления после каждой главы. А ведь раньше я мог читать час или два, не занимаясь чем-то еще. По работе мне приходится много писать, но если я пишу более длинные тексты, мне сложно оставаться сосредоточенным и эффективным».

Означает ли это, что от социальных сетей на работе следует отказаться всем людям, которые не связаны с ними профессионально?

«Я считаю, что социальные сети на работе – это хорошо, когда вам нужен перерыв, – комментирует Дженнифер Моррис. – Проблема заключается в зависимости: у нас действительно есть проблемы с ограничением этого времени».

(вгору)

Додаток 7

23.02.2019

Жертвы лайков. Почему дети боятся найти себя в Google и Instagram

Нравится ли современному ребенку, что мама выкладывает в Facebook и Instagram всю его жизнь – от снимка УЗИ до успехов в учебе (InternetUA)?

Дети растут быстро. Очень хочется запомнить, как сын или дочь делает первый шаг, говорит первое слово или первый раз ест ложкой суп, не обляпавшись. И возможность есть: сейчас даже простой смартфон

недурственно снимает фото и видео. Хронику взросления малыша можно вести непрерывно.

Штука в том, что поколение, выросшее в интернете, почти не представляет, как можно не запостить своих детей себе в соцсети. Тем более какое-то особенно удачное фото или забавное видео. Некоторые даже создают для своего ребенка отдельный аккаунт. Ничего же плохого в этом нет? Вон и друзья лайкают да умиляются в комментариях.

Но нравится ли самим детям, что вся их жизнь – от снимка УЗИ до смешных домашних выходок – выносится в онлайн?

Американская журналистка Тейлор Лоренц пообщалась по этому поводу с несколькими детьми и родителями. LIGA.net публикует адаптированный перевод статьи. И хотя текст заокеанский, для наших реалий тема не менее актуальна.

«Странно видеть себя там»

Здесь и далее имена детей заменены. Комментарии дети давали с разрешения родителей.

Кара несколько месяцев набиралась смелости, чтобы рассказать маме о том, что она увидела в Instagram. Не так давно 11-летняя девочка обнаружила, что большую часть ее жизни мама публиковала фотографии дочери без предварительного одобрения.

«Я хотела поднять этот вопрос. Странно видеть себя там, и иногда есть изображения, которые мне не нравятся», – говорит ребенок.

Как и большинство других современных детей, Кара «выросла» в социальных сетях. Facebook, Twitter и YouTube появились еще до ее рождения. Instagram развивался, начиная с ее младенчества.

У многих детей еще нет собственных учетных записей. Но их родители, школы, спортивные команды и организации управляют их присутствием в интернете с самого рождения.

«... задолго до того, как эти молодые люди открывают свое первое электронное письмо»

Недавно автор блога по воспитанию детей написала в эссе Washington Post о том, как много лет делилась очень личными историями о своей дочери в блоге и соцсетях. И даже когда 14-летняя дочь с ужасом это обнаружила и попросила прекратить, блогер уже не могла остановиться. Автор утверждает: пообещать дочери, что она перестанет публиковать информацию о ней, «будет означать закрытие важной части меня, что не обязательно хорошо для меня или для нее».

Таким страдают не только чрезмерно усердные мамы-блогеры. Многие обычные родители делают то же самое. Для этого даже есть термин: sharenting (шейринтинг – чрезмерное использование соцсетей для обмена контентом, основанного на детях – Ред.).

Согласно исследованию AVG, компании по обеспечению безопасности в интернете, почти четверть детей начинают свою цифровую жизнь, когда их родители загружают в интернет свои дородовые сонограммы. Исследование

также показало, что 92 % детей младше 2 лет уже имеют свои цифровые идентичности.

«Родители теперь формируют цифровую идентичность своих детей задолго до того, как эти молодые люди открывают свое первое электронное письмо. Раскрытие информации, которое родители делают онлайн, обязательно последует за их детьми во взрослую жизнь», – говорится в отчете University of Florida Levin College of Law.

«Даже если вы просто плаваете – мир об этом узнает»

Дошкольные и начальные школы часто ведут блоги или загружают фотографии детей в учетные записи Instagram и на страницы Facebook. Так работающие родители могут почувствовать себя более осведомленными о жизни своих малышей. Спортивные результаты записываются онлайн, как и знаковые моменты из внеклассных клубов.

Когда 11-летняя Эллен, наконец, решила сама попробовать Google, она не ожидала найти что-либо о себе – ведь никаких учетных записей в социальных сетях у нее не было. Она была ошеломлена, когда нашла в интернете результаты летних соревнований по плаванию и спортивную статистику. В 3 классе девочка написала личную историю – и обнаружила ее на сайте класса, подписанную ее именем.

Эллен сказала, что, хотя и не нашла ничего слишком чувствительного или личного, была разочарована тем, что вся информация о ней была размещена, по-видимому, без ее согласия.

«Неважно, что вы делаете – люди узнают об этом, – говорит она. – Даже если вы просто плаваете – мир об этом узнает. Мои достижения там – теперь люди знают, что я пловец. [Интернет] рассказывает, где занимаются плаванием, так что это, вероятно, расскажет о моем общем местоположении. И о моей школе. Части моей опубликованной истории были на испанском языке. Теперь люди знают, что я говорю по-испански».

«Это заставило меня почувствовать себя знаменитым»

Не все дети плохо реагируют на то, что без своего ведома живут онлайн. Некоторые даже в восторге от этого.

В четвертом классе Нейт поискал в Google свое имя. И обнаружил, что его упоминают в новостной статье о том, как его класс готовит гигантский буррито. Он очень удивился, но остался доволен своим новым влиянием.

«Это заставило меня почувствовать себя знаменитым... Я подружился с новыми ребятами, рассказав, что про меня написали в газете», – говорит Нейт. С тех пор он гуглит себя каждые несколько месяцев, надеясь что-то найти.

13-летняя Натали рассказывает, что в пятом классе она и ее друзья соревновались друг с другом за то, о ком в интернете больше информации. «Мы подумали, что это так круто, что у нас были свои фото в интернете», – говорит она.

Родители Натали строго не публикуют фотографии дочери в социальных сетях, поэтому там есть лишь несколько ее снимков. Но девочка жаждет большего.

«Я не хочу жить в норе с только двумя фотографиями в интернете. Я хочу быть человеком, который является человеком. Я хочу, чтобы люди знали, кто я», – говорит Натали.

«Все всегда смотрят, и ничто не забывается»

Кара и другие подростки говорят, что надеются установить правила для своих родителей. Кара хочет, чтобы мама рассказала ей в следующий раз, когда напишет о ней, и 11-летняя девочка хотела бы наложить вето на любую фотографию, прежде чем та появится в сети.

«Мои друзья всегда будут писать или говорить мне что-то вроде: “Боже мой, фотография, которую запостила твоя мама, такая милая”. И я буду очень стесняться», – говорит она.

10-летний Хейден несколько лет назад понял, что его родители использовали специальный хэштег с его именем для его фотографий. Теперь он следит за хэштегом, чтобы убедиться, что они не публикуют ничего смущающего.

Как только дети впервые осознают, что их жизнь публична, пути назад уже нет. Для нескольких подростков, с которыми общался The Atlantic, это стало стимулом, чтобы получить свои собственные профили в социальных сетях и попытаться взять под контроль свой интернет-образ. Но многие другие дети терпят поражение и отступают.

Эллен говорит, что всякий раз, когда рядом кто-то разговаривает по телефону, она нервничает: ее фотографию могут сделать и где-то выложить.

«Все всегда смотрят, и ничто не забывается. Оно никуда не исчезнет», – считает девочка.

«Мне не очень нравится, что люди знают обо мне, а я даже не знаю их»

Чтобы помочь детям ориентироваться в этой реальности, все больше начальных школ внедряют программы цифровой грамотности.

7-летняя Джейн рассказывает, что узнала о своем интернет-присутствии частично благодаря презентации о безопасности в интернете, которую проводили в школе. Ее отец также рассказал ей о социальных сетях и позволяет дочери утверждать фотографии, прежде чем они появятся в сети.

Тем не менее, Джейн беспокоится. Она слишком молода, чтобы самостоятельно ориентироваться в интернете. Но чувствует: многое из того, что есть в интернете о ней, находится вне ее контроля.

«Мне не очень нравится, что люди знают обо мне, а я даже не знаю их», – говорит Джейн.

Энди, которому тоже 7 лет, всегда настороже с людьми, которые могут его сфотографировать в неудобной ситуации. Однажды он поймал свою мать, которая сфотографировала, как он спит, а в другой раз - как исполняет смешной танец. Энди сразу же сказал ей не публиковать это в Facebook. По его ощущениям, фотографии его бы смутили.

«Тебе определенно нужно жить осторожно»

Некоторые законодательные органы также принимают участие в цифровой грамотности.

В 2014 году Верховный суд Европы постановил, что интернет-провайдеры должны предоставить пользователям «право быть забытым». В соответствии с этим решением, европейские граждане могут ходатайствовать о том, чтобы скрыть от результатов Google-поиска информацию из прошлого, наносящую ущерб. Включая преступления, совершенные в несовершеннолетнем возрасте.

Во Франции строгие законы о конфиденциальности означают, что дети могут подать в суд на своих родителей за публикацию интимных или личных подробностей их жизни без согласия. Однако в США детям и подросткам не предлагают такой защиты, и многие просто ходят по тонкому льду. «Тебе определенно нужно жить осторожно», – объясняет Эллен.

Джейми Патнем, мама из Джорджии, утверждает: она стала больше помнить, что многие из друзей ее детей еще не знают, сколько о них информации в сети.

Недавно она увидела в социальных сетях, что у одного из друзей ее ребенка появился щенок. Она сказала об этом, когда увидела мальчика в следующий раз, и он в ужасе посмотрел на нее. Он понятия не имел, как она узнала эту, казалось бы, личную информацию.

«Это заставило меня понять: эти дети не знают, что о них все время пишут, – говорит Джейми. Теперь она осторожна в том, что раскрывает. – Такое чувство, что ты, возможно, пересекаешь черту, рассказывая им все, что знаешь о них».

(вгору)

Додаток 8

24.02.2019
Ирина Фоменко
Соцсети для подростков опаснее каннабиса

В новаторском исследовании психиатр и доцент Калифорнийского университета в Сан-Диего Кара Багот изучает, влияют ли социальные сети на мозг подростка так же, как каннабис. Установление связи может изменить отношение медицинских работников к Instagram, Snapchat и другим соцсетям, пишет The Star Online (InternetUA).

«Психиатры не признают чрезмерное использование социальных сетей как аддиктивное поведение. Если исследование покажет аналогичные изменения в активации схемы вознаграждения мозга, то мы можем разработать модель лечения», – заявила Кара Багот.

Психиатр впервые сравнила социальные сети с каннабисом. «Уже есть исследования, которые показывают, что видеоигры, компьютерные игры, социальные сети и более широкое использование технологий связаны с плохими результатами в области физического и психического здоровья», – прокомментировала Багот.

Исследования

В опросе Pew Research Center, проведенном в 2018 году, 95 % молодых людей заявили, что у них есть смартфон, который чаще всего используется для доступа к социальным сетям. Более того, 89 % сообщили, что они были в сети «почти постоянно» или «несколько раз в день».

Опыт показывает, что использование социальных сетей дает некоторые преимущества. В то время как примерно шесть из десяти подростков испытали киберзапугивание, восемь из десяти настаивают на том, что социальные сети заставляют их чувствовать себя более связанными с друзьями.

Исследователи заметили интересную особенность: чем больше подростки используют социальные сети, тем чаще они откладывают получение водительских прав. Показатели употребления алкоголя, сигарет и запрещенных наркотиков несовершеннолетними падают.

«Если вы не общаетесь со своими сверстниками, вы склонны меньше употреблять наркотики», – считает Багот. – Дети все чаще общаются друг с другом в Интернете, а не в реальной жизни».

Тем не менее, исследования также связывают использование социальных сетей с депрессией, бессонницей и негативными образами тела. И хотя откладывание некоторых вещей (например, обучение вождению) может принести пользу обществу (и другим водителям), Баго задается вопросом, полезно ли это.

Четыре группы

Исследование Багот – небольшая часть масштабной инициативы по Когнитивному развитию мозга у подростков (ABCD), стоимостью 300 млн долларов, которая будет отслеживать около 12 000 детей в течение десятилетия. Это крупнейшее исследование, когда-либо проведенное среди молодых людей, было начато в 2015 году с участием экспертов из более чем 20 исследовательских институтов, включая Калифорнийский университет в Сан-Диего.

Когда стартовала инициатива ABCD, ректор Калифорнийского университета Сандра Браун предположила, что это может «привести к новым подходам к образованию и типам вмешательств для решения общих проблем, возникающих в подростковом возрасте».

«Новый подход» планирует использовать Баго: сканировать мозг подростков при просмотре изображений марихуаны, наркотических принадлежностей и постов в Instagram. Исследователи будут изменять последнее, добавляя или убирая «лайки», чтобы вызывать положительные или отрицательные эмоции. Изображения, полученные с помощью функциональной МРТ, покажут, светиться ли та же часть мозга при просмотре фото марихуаны и постов в Instagram.

60 подростков поделят на четыре группы – заядлые потребители и любители марихуаны; активные и малоактивные пользователи социальных сетей. Средства на исследование Баго получит уже этой весной, поэтому результаты будут готовы к концу года.

По словам профессора, обучение относительно социальных сетей должно продолжаться и дальше. «Мы должны научить детей быть хорошими распорядителями собственной информации. Они не понимают, что оставляют цифровой след», – прокомментировала Баго, сославшись на случаи, когда старые посты в Instagram или Facebook приводили к отмене предложений о работе.

(вгору)

Додаток 9

18.02.2019

Как не попасться на фейки в соцсетях и новостях: украинцам дали важные советы

Любой читатель, слушатель и просто посетитель Сети может запросто утонуть в океане информации. Те, кто владеет СМИ, уже давно используют этот бесконечный поток фактов, новостей, изображений и видео, чтобы манипулировать «беззащитным Фомой». Поэтому так важно знать правила распознавания фейков, говорится в сообщении посольства США в Украине (InternetUA).

«Эта информационная война не прекращается ни на миг, принося преимущества злоумышленникам, создавая фантомы и мифы, вынуждая массы людей верить в них. Вот почему сейчас такой важной является медиаграмотность, возможность противостоять атакам, выводя авторов на чистую воду правды», – говорится в видеообращении.

Опираясь на опыт американских СМИ, авторы ролика приводят шесть важных правил того, как распознать фейки в соцсетях и новостях.

1. Не доверяйте заголовку, читайте саму статью

Очень часто заголовок создается для того, чтобы перекрутить факты, обратить внимание на что-то другое, переключить внимание на нечто выгодное манипуляторам. Или даже «загрузить мозг чепухой», которая усилит образ ненавистного врага. Только содержание может выяснить правдивость заголовка.

2. Не доверяйте подозрительном источнику, особенно если он единственный

Если провести нехитрые исследования, можно установить степень заангажированности автора информации. Если источник единственный, подозрение в манипуляции имеет все основания. Как правило, важная новость дублируется всеми признанными источниками.

3. Не верьте неизвестным экспертам

На самом деле этих людей мало кто знает не только в широких кругах, но и в «очень узких». Эти так званые «аналитики» выполняют задания манипуляторов и обычно исчезают из поля зрения через некоторое время. Людей, чье мнение имеет значение, в обществе хорошо знают и уважают.

4. Проверяйте дату информации

Довольно распространенным способом манипуляции является размещение информации, актуальность которой уже прошла. И появление ее в сегодняшнем потоке новостей имеет цель, понятную только манипуляторам-хитрецам.

5. Не верьте глазам своим: не все, что на фото – правда

Наукой установлено, что наше зрение воспринимает больше информации, чем наш слух. Настоящим «другом» фейка является фотошоп, с помощью которого на фотографию добавляют все, что было снято не там, не в том месте и не по той причине.

6. Помните, что не все, что движется и звучит на экране – реально

Возможно, что перед вами всего лишь «созданная» реальность или «перемонтированная» реальность. Действующие лица могут быть реальными, а их слова и действия – нет. Место события может быть реальным, а само событие – нет. И наоборот.

«Будем более внимательны, не дадим недоброжелателям сделать из нас покорных зомби. Помните, что информационная война за наши головы и сердца идет круглые сутки. И только от нас лично зависит противодействие и сопротивление этим атакам», – резюмируют свое обращение авторы ролика.

(вгору)

Додаток 10

18.02.2019

Ирина Фоменко

Alibaba разработала пропагандистское приложение для правительства Китая

Пропагандистское приложение китайского правительства, которое недавно стало хитом, было разработано Alibaba. Об этом сообщает The Star Online (InternetUA).

Xuexi Qiangguo, что буквально переводится как «Учения, чтобы сделать Китай сильным» – приложение на правительственную пропагандистскую тему о применении идей президента Си Цзиньпина. Xuexi Qiangguo обогнала Tik Tok и WeChat, став самой популярной программой в китайском Apple Store на прошлой неделе.

Приложение разработала команда по специальным проектам в Alibaba – «Y Projects Business Unit». Xuexi Qiangguo стало последним примером сотрудничества китайской технологической компании с правительством.

Отдел пропаганды страны выпустил приложение в преддверии Национального народного конгресса в Пекине, который состоится в следующем месяце – крупнейшего ежегодного парламентского собрания Китая.

Предложения работы

В приложении есть короткие видеоролики, правительственные новости и викторины. Пользователи DingTalk могут использовать свои учетные данные

для входа в Xuexi Qiangguo. В Alibaba заявили, что приложение разработано с использованием программного обеспечения DingTalk.

Сотрудники отдела Alibaba отвечают за разработку и поддержку приложения, сообщается на веб-сайте компании по поиску работы. У этого подразделения нет своего ресурса, но их работа описана в объявлениях о вакансиях на популярном китайском сайте Zhipin.com как проект стратегического уровня, находящийся на стадии создания и предлагающего множество возможностей трудоустройства.

По крайней мере, часть популярности приложения можно объяснить директивами, изданными местными органами власти и университетами, которые требуют, чтобы члены партии Китая загружали программу.

По оценкам пекинской статистической консалтинговой компании Qimai, приложение загрузили более 43,7 млн раз на устройства Apple и Android с начала этого года.

Обширное сотрудничество

Крупные китайские технологические компании активно сотрудничают с правительством в области инфраструктуры, облачных вычислений и общественной безопасности в рамках политики страны Internet Plus, направленной на улучшение традиционных отраслей.

Партнерство со СМИ также возросло в последние годы на фоне ужесточения законов о цензуре, которые требуют от предприятий придерживаться партийной линии.

Создатель Tik Tok Beijing ByteDance Technology Co и основатель WeChat Tencent Holdings Ltd являются одними из тех, кто сотрудничал с государственными СМИ, используя свои платформы социальных сетей.

«Преимущество этих фирм в том, что их опыт сотрудничества может помочь получить ключевые лицензии или возможности. Недостаток – их могут привлечь к участию в проектах, которые, исходя только из экономических соображений или связей с общественностью, они обычно избегают, но от них может быть неудобно или неразумно отказываться», – заявил управляющий директор Marbridge Consulting Марк Наткин. По его мнению, партнерство такого рода было способом правительства Китая сохранить контроль над частными компаниями.

(вгору)

Додаток 11

21.02.2019

В НАТО перевірили стійкість військових до провокацій у Facebook

Дослідницька група Центру передового досвіду Стратегічних комунікацій НАТО створила низку фейкових акаунтів від імені військових. Мета – перевірити, наскільки фейкові облікові записи зможуть вплинути на реальні дії солдатів за допомогою маніпуляцій у соціальних мережах. Зокрема, у Facebook та Twitter (InternetUA).

«Ми спробували відповісти у нашому експерименті на три запитання, – каже Нора Бітеніс (Nora Biteniece), інженерка-програмістка проекту, виданню Wired. – Що ми можемо дізнатися про військові навчання лише з відкритих даних? Що ми зможемо дізнатися про їхніх учасників? І чи можна використовувати всі ці дані для повстання солдатів проти наказів керівництва?».

Протягом чотирьох тижнів дослідники розробляли фальшиві сторінки та закриті групи на Facebook, а також профілі користувачів-військових, які уособлювали як реальних осіб, так і вигаданих. Аби спровокувати військових відвідати ці групи, дослідники використали таргетовану рекламу. Бюджет – всього $60, що робить подібні прийоми особливо доступними для тролів та провокаторів. Фейки розпитували справжніх військовослужбовців про атмосферу у їхніх батальйонах та особливості роботи. Функція «Рекомендованих друзів» на Facebook допомагала дослідникам знаходити нових «жертв» та виявляти їхнє коло спілкування.

Спеціалісти також відстежували облікові записи у Twitter та в інших відкритих джерелах, які могли б використати зловмисники. «Нам вдалося знайти багато даних про наших піддослідних і деякі з них були доволі інтимними, – каже Бітеніс. – Наприклад, деякі одружені військові виявилися поціновувачами сервісів для романтичних знайомств».

Наприкінці експерименту дослідники ідентифікували 150 військовослужбовців, знайшли місця розташування декількох батальйонів, відстежили рухи військ і змусили деяких військових покинути свої службові пости супроти наказів керівництва.

«У кожної людини є свій внутрішній важіль. Для когось це фінанси, для когось це довгоочікуване побачення, для когось це родина, – каже Яніс Сартс (Janis Sarts), директор Центру передового досвіду Стратегічних комунікацій НАТО. – Інтернет дозволяє натиснути на цей важіль, бо надає про вас детальну інформацію».

Представник Facebook заявив, що компанія «вітає зусилля дослідників, які інформують керівництво соцмереж про свої висновки». Також співрозмовник Wired порекомендував не приймати підозрілі запити на додавання у друзі та повідомляти службу підтримки про випадки вивідування приватної та конфіденційної інформації.

(вгору)

Додаток 12

24.02.2019

Цукерберга «викликали на килим» борці з фейками та дезінформацією

Члени Міжнародного комітету із питань дезінформації й фейкових новин запросили на засідання у парламенті Канади власника Facebook Марка Цукерберга та керівників інших соцмереж (Espreso.tv).

За словами члена Міжнародного комітету від Канади, депутат федерального парламенту Роберта Цимера, запрошення долучитися до засідання, що відбудеться наприкінці травня у Оттаві, окрім Цукерберга, отримали головний операційний директор Facebook Шеріл Сандберг, генеральний директор Google Сандар Пічай та колишній глава ради директорів компанії Ерік Шмідт, генеральний директор Apple Тім Кук та головний операційний директор компанії Джеф Вільямс, генеральний директор Amazon Джеф Безос, генеральний директор Twitter Джек Дорсі, співзасновник WhatsApp Браян Актон і генеральний директор Snap Inc. Еван Шпігель.

«Сподіваюся, ці керівники скористаються унікальною можливістю поспілкуватися із представниками держав з усього світу про те, що їх платформи роблять для збереження приватності наших громадян», – сказав Цимер, який очолює Постійний комітет із питань доступу до інформації, приватності та етики парламенту Канади.

Він додав, що очікує також почути від запрошених що робиться для припинення поширення дезінформації та для захисту користувачів від загрози онлайн маніпуляцій.

«Ми не приймемо свідчень регіональних представників на цій зустрічі, оскільки попередній досвід показує, що їх відповіді є неадекватними», – зазначив Цимер.

Міжнародний комітет складається із депутатів з Канади, Великої Британії, Аргентини, Бельгії, Бразилії, Франції, Ізраїлю, Латвії та Сингапуру. Перше його засідання відбулося у листопаді минулого року в Лондоні. Марк Цукерберг тоді відмовився брати у ньому участь, надіславши замість себе віце-президента Річарда Алана, що викликало обурення парламентаріїв.

17 лютого стало відомо, що Facebook закидають шпигунство за «потенційно небезпечними» користувачами за допомогою IP-адрес.

(вгору)

Додаток 13

14.02.2019
Ирина Фоменко
Что такое кибератака «посредника» и как ее предотвратить

Атака посредника или «человек посередине» (man-in-the-middle, MitM) – когда злоумышленник перехватывает связь между двумя сторонами, либо тайно подслушивает, либо изменяет трафик, проходящий между ними. Хакеры могут использовать атаки MitM для кражи учетных данных или личной информации, шпионажа за жертвой, диверсии коммуникации или искажения данных, пишет IT News (InternetUA).

«Атаки MitM являются тактическим средством для достижения цели, которая может заключаться в шпионаже за отдельными лицами или группами для перенаправления усилий, средств, ресурсов или внимания», – пояснил технический стратег CrowdStrike Зеки Туриди.

Хотя от MitM можно защититься с помощью шифрования, злоумышленники могут перенаправлять трафик на фишинговые сайты либо передавать его к месту назначения или регистрации, что делает обнаружение подобных атак невероятно сложным.

Как работают атаки MitM?

Атаки MitM подразумевают «посредника» между соединением двух сторон, наблюдение за трафиком или манипулирование им. Это может быть вторжение в законные сети или создание поддельных, которые будет контролировать злоумышленник.

Скомпрометированный трафик затем удаляется из любого шифрования для кражи, изменения или перенаправления этого трафика к месту назначения (фишинговый сайт). Поскольку злоумышленники могут повторно шифровать перехваченный трафик, обнаружить подобную атаку крайне сложно.

«MitM-атаки – когда злоумышленник фактически находится между жертвой и законным хостом, к которому пытается подключиться пострадавший. Таким образом, хакер либо пассивно прослушивает соединение, либо перехватывает его, завершает и устанавливает новое соединение с пунктом назначения», – заявил декан Технологического института SANS Йоханнес Ульрих.

MitM включает в себя широкий спектр методов и потенциальных результатов, в зависимости от цели и задачи. Например, при разборке SSL злоумышленники устанавливают соединение HTTPS между собой и сервером, но с незащищенным HTTP-соединением с пользователем – информация отправляется в виде простого текста без шифрования.

Атаки Evil Twin отражают действительные точки доступа Wi-Fi, но полностью контролируются злоумышленниками, которые теперь могут отслеживать, собирать или манипулировать всей информацией пользователя.

«Эти типы атак могут быть направлены на шпионаж или финансовую выгоду. Наносимый ущерб варьируется от маленького до огромного, в зависимости от целей атакующего и способности причинять вред», – прокомментировал Туриди.

В случае с банками злоумышленник видит, что пользователь совершает перевод, и меняет номер целевого счета или отправляемую сумму. Хакеры используют MitM-атаки для сбора личной информации или учетных данных.

Если злоумышленники обнаруживают загрузку или обновление приложений, они устанавливают вредоносное ПО вместо законного. Набор эксплойтов EvilGrade был разработан специально для плохо защищенных обновлений. Учитывая, что им часто не удается зашифровать трафик, мобильные устройства особенно подвержены риску.

«Эти атаки могут быть легко автоматизированы. Существуют инструменты для автоматизации, которые ищут пароли и записывают их в файл, а потом отправляют вредоносный трафик обратно», – объяснил Ульрих.

Несмотря на то, что часто атаки по Wi-Fi или физической сети требуют близости к жертве, также возможно удаленное нарушение протоколов маршрутизации.

«Это более сложная и изощренная атака. Злоумышленники могут объявить себя в Интернете ответственными за эти IP-адреса, затем Интернет направляет их преступнику, после чего хакеры снова запускают MitM-атаки», – заявил Ульрих. – «Они также могут изменять настройки DNS для определенного домена. Если вы переходите на определенный веб-сайт, то на самом деле подключаетесь IP-адресу злоумышленника – так преступник может начать атаку “человек посередине”».

MitM-атаки можно проводить через поддельные вышки сотовой связи. Правоохранительные органы в США, Канаде и Великобритании использовали их для массового сбора информации. Исследователи из Технического университета Берлина, ETH Zurich и SINTEF Digital в Норвегии недавно обнаружили уязвимости в протоколах Authentication and Key Agreement (AKA), используемых в 3G, 4G и 5G, которые могут привести к выполнению хакерами MitM-атак.

Насколько распространены MitM-атаки?

Хотя атаки MitM не так распространены, как вирусы-вымогатели или фишинговые атаки, они представляют собой постоянную угрозу для организаций. В документе IBM X-Force Threat Intelligence Index 2018 сообщается, что 35 % эксплуатации включали MitM-атаки.

«Я бы сказал, основываясь на неподтвержденных данных, что атаки MitM не сильно распространены. Многих целей – слежка за данными/коммуникациями, перенаправление трафика – можно достигнуть с помощью вредоносных программ, установленных в системе жертвы. Если есть более простые способы выполнения атак, противник часто выбирает легкий путь», – заявил аналитик разведки угроз Palo Alto Networks Алекс Хинчлифф.

Примечательным недавним примером была группа российских агентов ГРУ, которые пытались взломать офис Организации по запрещению химического оружия (ОЗХО) в Гааге, используя спуфинговое устройство Wi-Fi.

В 2017 году в Electronic Frontier Foundation (EFF) заявили, что более половины всего интернет-трафика теперь зашифровано, а Google – что в некоторых странах более 90 %. Основные браузеры, такие как Chrome и Firefox, также будут предупреждать пользователей, если они подвергаются риску MitM-атак.

«С ростом применения SSL и появлением современных браузеров атаки MitM стали менее популярными. Принципы MitM используют в очень сложных атаках. Один из примеров – вредоносное ПО, нацеленное на сеть SWIFT крупной финансовой организации, в которой использовался метод MitM для создания ложного баланса счета, поскольку средства пересылались на счет киберпреступника», – поделился Туриди.

Однако угроза все еще существует. Например, банковский троян Retefe перенаправляет трафик с банковских доменов через серверы, контролируемые

злоумышленником, расшифровывая и изменяя запрос перед повторным шифрованием данных и отправкой их в финучреждение. Недавно обнаруженный недостаток протокола TLS, включая новейшую версию 1.3, позволяет злоумышленникам нарушать RSA и перехватывать данные.

Предотвращение MitM-атак

Протоколы шифрования, такие как TLS, являются лучшим способом защиты от атак MitM. Последняя версия TLS стала официальным стандартом в августе 2018 года. Есть и другие, например, SSH или более новые протоколы – QUIC от Google.

В целях обучения поощряйте персонал:

- не использовать открытый Wi-Fi или Wi-Fi в общественных местах, поскольку такие соединения легче взломать;
- прислушиваться к предупреждениям браузеров о том, что сайты или соединения незаконны;
- использовать VPN для обеспечения безопасности соединений.

«Лучшие методы включают многофакторную аутентификацию, максимальное управление сетью, видимость, а также сегментирование вашей сети», – заявил Хинчлифф.

Эксперты считают, что лучше предотвратить атаку, чем после – исправлять ситуацию. «Эти атаки трудно обнаружить большинству традиционных устройств безопасности», – прокомментировал Туриди.

Если квантовая криптография станет коммерчески жизнеспособной, она может обеспечить надежную защиту от MitM-атак: невозможно копировать квантовые данные, нельзя их контролировать, не изменив состояние, и, следовательно, предоставить надежный индикатор, если трафик подвергается вмешательству.

Является ли Интернет вещей следующей границей для атак MitM?

Аналитики прогнозируют, что количество устройств, подключенных к Интернету, может вырасти до десятков миллиардов в течение следующих пяти лет. К сожалению, отсутствие безопасности во многих устройствах означает, что рост числа IoT-девайсов привет к скачку атак MitM.

«IoT-устройства, как правило, более уязвимы для взломов, потому что они не реализуют стандартные меры по защите от MitM-атак. Многие IoT-девайсы еще не используют TLS», – заявил Ульрих.

Новое исследование, проведенное Институтом Ponemon и OpenSky, показало, что 61 % специалистов по безопасности в США говорят, что не могут контролировать распространение устройств IoT и IIoT в своих компаниях, в то время как 60 % – что они не могут избежать взломов безопасности и нарушений данных, связанных с IoT и IIoT.

(вгору)

Додаток 14

14.02.2019

Современный умный дом – сплошная дыра в безопасности

Состояние безопасности в инфраструктуре умного дома – не просто плохое, а очень плохое. Ежегодно к сети подключаются миллионы новых устройств, разработчики которых попросту забыли подумать о защите (IGate).

Иногда проблемными оказываются даже устройства именитых производителей, вроде Xiaomi. Хакерам Limited Results удалось извлечь из популярных смарт-лампочек LIFX, Xiaomi, Tuya и WIZ пароли от Wi-Fi. Как выяснилось, пароли хранились там в совершенно незашифрованном виде. Правда, чтобы извлечь данные, хакеру пришлось вскрыть лампочку физически. Но это – все равно уязвимость. Ведь взломщик, желающий заполучить доступ к вашей домашней сети, может извлечь сгоревшую лампочку из мусорного бака.

Эксперт по безопасности и основатель компании VTrust Михаэль Штайгервальд смог взломать умную лампочку Tuya удаленно, без вскрытия. Процесс взлома Штайгервальд продемонстрировал лично на одной из своих лекций в Лейпциге.

В целом же, проблема инфраструктуры умного дома является глобальной и не касается отдельных производителе или определенного типа устройств.

Кому можно доверять?

Эксперты AndroidPit пообщались о проблеме с представителем компании AV-Test Майком Моргенштерном. Они спросили, как может потребитель заранее знать, заслуживает ли то или иное устройство доверия. По словам Моргенштерна, общая ситуация не предрасполагает к доверию.

«Общество обращает внимание, прежде всего, на те случаи, в которых явно что-то пошло не так. Но в этой ситуации самым пугающим является то, что одни и те же простые ошибки совершаются снова и снова, чего быть не должно. Часто в сложном взломе нет никакой необходимости, ведь пароли просто пересылаются по сети в виде открытого текста.

С 2013 года мы тестируем устройства интернета вещей и выявили несколько тенденций. Известные производители прилагают все больше усилий, чтобы гарантировать информационную безопасность, так что мы видим, как ее уровень постоянно повышается. Но в то же время новые компании постоянно прибывают на рынок, и для них безопасность зачастую не играет важной роли. Кроме того, подход к защите данных может быть очень разным.

Европейские производители все чаще привлекают внимание основательным подходом к безопасности и разумными требованиями к защите данных. Если компании также проходят добровольный тест безопасности, вроде AV-TEST, их продукты получают отметку «TESTED SMART HOME PRODUCT» [«Проверенный продукт умного дома», – прим. ред.]. В этом случае есть высокие шансы, что устройством можно пользоваться безопасно и что данные пользователя не будут скомпрометированы», – рассказывает Моргенштерн.

Следует также учитывать, что небезопасные технологии могут использоваться в продуктах самых разных компаний. К примеру, та же Tuya продает компоненты тысячам более мелких производителей. По словам самих

представителей Tuya, их клиентами являются около 10 тыс. компаний по всему миру. Конечно, после того, как Михаэль Штайгервальд уличил Tuya в пренебрежении к безопасности, производитель начал принимать меры. По словам представителей компании, уже сделано или будет сделано в ближайшее время следующее:

– AES-ключи будут передаваться в зашифрованном виде;

– соединение устройств с облаком Tuya будет шифроваться по протоколу TLS;

– информация во флэш-памяти будет также храниться в зашифрованном виде;

– программное обеспечение будет проверяться;

– мобильные приложения получат дополнительные опции управления безопасностью.

К сожалению, как показывает практика, данные о местоположении каждого отдельного пользователя все еще могут быть восстановлены из облака Tuya. А значит, всем производителям, использующим технологии той компании, может быть известно о своих потребителях больше, чем следовало бы. И, как уже говорилось, сами потребители об этом даже не догадываются.

Производитель лампочек Lifx недавно тоже пообещал, что начнет уделять больше внимания безопасности. Компания Xiaomi тоже выпустила соответствующий патч. Это уже неплохо. Жаль лишь, что для этого каждого из производителей пришлось сначала «поймать за руку».

Как быть простому пользователю?

Если вы заинтересовались инфраструктурой умного дома и хотите к ней приобщиться, забудьте о том, чтобы просто пойти и купить гаджеты, которые вам нравятся. Возможно, так можно будет поступать в будущем – лет через пять-десять. Сейчас же такое поведение является слишком безрассудным. Пользование многими из устройств, которые присутствуют сегодня на рынке, попросту небезопасно.

Для начала пользователю следует углубиться в вопрос и тщательнее изучить предложение. Обращайте внимание не только на сам товар, но и на то, что о нем пишут в сети. Пожалуй, не следует покупать новые устройства от компаний, которые лишь недавно вышли на рынок.

Скандалы, как ни удивительно, могут быть хорошим признаком. Если какого-то производителя публично уличили в плохой безопасности и он выпустил соответствующее обновление, вы можете быть уверены в том, что конкретно эту дыру уже залатали. А вот если малоизвестный продукт вовсе не попадал в поле зрения экспертов-безопасников, то, возможно, в нем еще полно уязвимостей, которые пока никто не заметил.

(вгору)

Додаток 15

15.02.2019

Тысячи приложений для Android уличили в незаконной слежке

Вопреки усилиям, которые Google прикладывает для искоренения потенциально опасных приложений из Google Play, порядка 17 тысяч программ для Android ведут сбор информации о пользователях, даже если им запретили это делать. Такой вывод сделали исследователи Международного института компьютерных наук, изучив ассортимент фирменного каталога поискового гиганта. Впоследствии полученные данные используются рекламодателями для демонстрации релевантной рекламы, но иногда могут быть перепроданы на сторону (Украинский телекоммуникационный портал).

Примерно треть от общего числа приложений, ведущих слежку вопреки воле пользователя, делают это в интересах рекламодателей. Они формируют виртуальный портрет пользователя и на основе информации о его дейтвиях в Сети выстраивают персонифицированную рекламную подборку. Но есть, впрочем, и такие приложения, которые собирают такие сведения, как MAC-адрес, IMEI и Android ID, не подлежающие изменению и позволяющие при желании деанонимизировать любого пользователя, вычислив его из миллионов других.

Приложения-шпионы для Android

«Конфиденциальности приходит конец, когда приложения собирают такие данные, – говорит Серж Эгельман, руководитель исследования. – Они позволяют вычислить конкретного пользователя. Мы сообщили о результатах исследования в Google, уточнив, что большая часть изученных нами приложений действуют в нарушение политики конфиденциальности, установленной в Google Play».

Официальные представители Google отреагировали на исследование и заявили, что прикладывают все усилия для обеспечения безопасности своих пользователей. Тем не менее, признаются в компании, они могут контролировать отправку только тех данных, которые поступают на сервера собственных рекламных служб Google. В случаях, если приложение направляет информацию на внешние сервера, деятельность которых контролируется независимым предприятием, поисковый гигант не имеет какой-либо власти.

(вгору)

Додаток 16

18.02.2019

Новый троян использует антивирусы для кражи данных

ИБ-эксперты Cybereason Nocturnus Research обнаружили новую версию малвари Astaroth, которая использует легитимные процессы (в том числе и защитного ПО) в своих целях. Исследователи пишут, что троян использует продукты Avast и GAS Tecnologia для хищения данных и загрузки вредоносных модулей (InternetUA).

Инфостилер Astaroth был замечен специалистами еще в 2018 году. К примеру, о малвари рассказывали аналитики компании Cofense. Тогда, как и

сейчас, Astaroth атаковал пользователей в Бразилии и странах Европы, и задействовал для работы легитимные решения, к примеру, эксплуатировал интерфейс командной строки WMIC для тайной загрузки и установки вредоносных пейлоадов.

Astaroth способен похищать данные из буфера обмена, перехватывать нажатия клавиш, системные сообщения, похищать учетные данные от различных служб и сервисов, а также стремится собрать как можно больше информации о зараженной системе и финансовых счетах жертвы.

Новая вариация Astaroth, обнаруженная Cybereason Nocturnus Research, похожа на своих «предшественников», и тоже использует в работе легитимную утилиту Windows BITSAdmin для загрузки пейлоадов. Как и в предыдущих случаях, троян распространяется через спамерские письма и доставляется на машину жертвы во вложении (файл .7zip) или через вредоносную ссылку в таком письме.

Также исследователи заметили, что данная версия трояна осуществляет инжект вредоносного модуля в процесс aswrundll.exe (Avast Software Runtime Dynamic Link Library), принадлежащий антивирусу Avast. С его помощью троян извлекает данные с зараженной машины, а также загружает дополнительные модули, если потребуется. Если же Avast в зараженной системе отсутствует, аналогичный «трюк» малварь проделывает с процессом unins000.exe, принадлежащим защитному решению компании GAS Tecnologia.

После публикации отчета Cybereason Nocturnus Research представители Avast связались с исследователями и СМИ и пояснили, что защитное ПО компании не подвергается взлому, а действия преступников не являются инжектами или эскалацией привилегий. Разработчики заверили, что уже изучают проблему и в ближайшее время введут новые защитные меры, чтобы предотвратить подобные злоупотребления в будущем.

(вгору)

Додаток 17

18.02.2019

Хакеры нашли способ обмануть даже самых бдительных пользователей

Как правило, пользователи, заботящиеся о безопасности собственных данных, прежде чем ввести логин и пароль в форму авторизации на каком-либо сайте, обращают внимание на несколько факторов, например, корректность URL и реализацию HTTPS на сайте или используют различные браузерные расширения, определяющие фишинговые домены. Однако недавно эксперты заметили новую фишинговую кампанию, которая может ввести в заблуждение даже самых бдительных пользователей (InternetUA).

По словам специалиста компании-разработчика менеджера паролей Myki Антуана Венсана Жебара (Antoine Vincent Jebara), злоумышленники распространяют ссылки на блоги и сервисы, где пользователям сперва

требуется зарегистрироваться через учетную запись в Facebook для того, чтобы прочитать публикацию или приобрести товар по скидке.

Практика регистрации через Facebook или другие соцсети используется многими сайтами для упрощения регистрации в стороннем сервисе. Обычно при нажатии на опцию «Вход через Facebook» происходит либо переадресация на сайт facebook.com или в окне браузера появляется всплывающее окно, где нужно ввести учетные данные для аккаунта в Facebook для аутентификации и разрешения сервису получить доступ к нужной информации в профиле.

Как обнаружил эксперт, вредоносные блоги и online-сервисы после выбора опции «Вход через Facebook» предлагают пользователям весьма реалистично выглядящую фальшивую форму авторизации Facebook, собирающую введенные логин и пароль (так же, как и любой другой фишинговый сайт).

Как видно в демонстрационном видео ниже, фальшивая всплывающая форма, созданная с помощью HTML и JavaScript, является отличной имитацией окна в браузере, включая строку состояния, панель навигации, URL и даже зеленый замок, указывающий на использование HTTPS. Более того, пользователи даже могут взаимодействовать с окном, перетаскивать его в разные стороны или закрыть его так же, как и легитимные окна.

Единственная возможность распознать подложное диалоговое окно – попробовать перетащить его за пределы окна в браузере, в котором оно отображается. Фальшивое окно перетащить не получится, поскольку оно является частью вредоносной страницы, пояснил специалист.

(вгору)

Додаток 18

19.02.2019

Google запретит сайтам следить за пользователями

Google решил усилить защиту пользователей в режиме инкогнито, который в теории позволяет людям посещать сайты, не оставляя электронных следов. Однако некоторые веб-страницы научились обходить встроенную в браузер Chrome систему безопасности – они обнаруживают, что человек включил специальный режим и блокируют его использование (U-News).

Специалисты 9to5Google на днях обнаружили на сайте управления исходным кодом Chromium Gerrit сегменты, которые свидетельствуют о подготовке поисковым гигантом исправления, призванного закрыть обнаруженную прореху.

Некоторые сайты, предлагающие платную подписку после пробного периода, давно смекнули, что пользователи с легкостью обходят требование об оплате, входя на страницу в анонимном режиме. Коль скоро система не может идентифицировать посетителя, она позволяет ему бесплатно пользоваться ресурсом.

Победить слишком «умных» пользователей, впрочем, оказалось не так уж сложно. Дело в том, что в режиме инкогнито Chrome отключает свой API «Файловая система». Понимая, что он выключен, сторонний сайт может с точностью определить, что пользователь зашел на веб-страницу анонимно и запретить ему просмотр контента.

Прогнозируется, что исправление этой особенности произойдет уже в версии Chrome 74 Canary, который должен состояться 23 апреля. Но первое время ее нужно будет активировать самостоятельно. По умолчанию исправление начнет работать в более поздней сборке браузера – Chrome 76 в конце июля 2019 года.

(вгору)

Додаток 19

20.02.2019

YouTube vs педофилия: скандал ElsaGate вне времени

В 2017 году YouTube попал в скандал ElsaGate и в 2019 он снова набирает обороты (Телекритика).

После ролика блогера Мэтта Уотсона, где он утверждает, что видео с детьми привлекает внимание педофилов, которые свободно общаются в комментариях и обмениваются ссылками на детское порно, и к тому же эти видео монетизируются, YouTube попал в очередной скандал.

Мэтт Уотсон сообщает, что подобные видео помогают педофилам организовывать свое сообщество, обмениваться контакты и ссылками. К примеру при запросе «bikini haul» (выбор купальников) YouTube практически сразу рекомендует видео с детьми. Там нет ни эротики, ни пошлости, но само присутствие ребенка в кадре толкает больное воображение педофилов на комментарии, касающиеся движений и поз детей. Нередко под видео можно встретить ссылки на сайты с запрещенным контентом.

«Алгоритм рекомендаций YouTube облегчает педофилам возможность общаться с себе подобными в комментариях, обмениваться контактной информацией и ссылками на фактически детскую порнографию. Я могу получить доступ туда с только что созданного аккаунта менее чем за десять минут, для этого нужно всего лишь несколько кликов», – написал Мэтт Уотсон на Reddit.

Помимо этого, видеоплатформа монетезирует некоторые ролики. На них появляется реклама часто с жестокими и отвратительными сценами. В 2017 году скандал получил название ElsaGate. Тогда же YouTube обновил правила публикации контента и закрыл возможность оставлять комментарии к видео с детьми, чтобы пресечь действия педофилов, но сервису так и не удалось выработать эффективный способ решения этой проблемы.

Нельзя сказать, что YouTube равнодушен к существующей проблеме. Он тесно сотрудничает с правоохранительными органами, с Национальным центром по проблемам пропавших без вести и подвергающихся эксплуатации

детей (NCMEC) и неправительственной организацией для надзора за интернетом Internet Watch Foundation (IWF). Единственное, что может предпринять YouTube в случае с детским контентов – это закрыть комментарии, лишив ненормальных возможности высказать свое «мнение».

(вгору)

Додаток 20

20.02.2019

У зашифрованих месенджерах продають дитяче порно – розслідування BBC

Безкоштовні шифровані додатки для обміну повідомленнями Telegram і Discord опинилися у центрі скандалу. Ці месенджери мають як відкриту, так і приховану сторону – і зловмисники користуються цим для розповсюдження заборонених матеріалів, пише BBC. Серед них – групи з продажу наркотиків, вкрадених фінансових даних та дитячої порнографії (InternetUA).

Зловмисники використовували і Telegram, і Discord, аби надати користувачам доступ до матеріалів з дитячою порнографією та знущаннями над дітьми. Посилання на такі групи у Telegram знаходилися у коментарях під відео на YouTube. Коментарі містили кодові слова, які користувач міг вільно вбити у пошуковик та отримати посилання на заборонений контент прямо з пошукової видачі. Після натискання на лінк користувач переходив у закритий чат чи канал. І хоча «публічна» сторона цього каналу була формально доступна в Інтернеті, після переходу в чат чи групу дані ставали зашифрованими.

Дослідники підтвердили, що принаймні одна з викритих груп містила сотні непристойних зображень дітей.

У YouTube заявили, що компанія рішуче блокує будь-які згадування подібного контенту на своїй платформі та вкладає кошти у технології для вирішення цієї проблеми. Представник Telegram заявив, що компанія обробляє відгуки користувачів та проводить «попереджувальні пошуки» для захисту платформи від подібних матеріалів та пропаганди тероризму.

Розслідування BBC показало, що зловмисники також використовують додаток Discord. Автори виявили низку групових чатів, які позиціонували себе як постачальники дитячого контенту для аудиторії від 13 до 17 років. Насправді ж метою шахраїв було переконати дітей надсилати у ці чати свої інтимні фото.

Аріель Ейнхорен (Ariel Ainhoren), керівник відділу досліджень в охоронній фірмі IntSights, розповів про торгівлю такими фотографіями. «Один зі зловмисників пропонував гігабайти порно для педофілів за гроші. 9 гігабайт за $50, 50 гігабайт за $500, і 2,2 терабайта за ціною близько $2500", – говорить Ейнхорен.

Представники Discord відповіли, що кількість таких порушень становить невеликий відсоток від всього трафіку додатку, і команда розробників працює над його мінімізацією.

(вгору)

Додаток 21

20.02.2019

Пользователи Android не могут отличить поддельные приложения от настоящих

Вредоносные приложения для Android, списывающие деньги с карт своих жертв, представляют даже меньшую опасность, чем поддельные банковские приложения. Такой вывод сделал исследователь в области кибербезопасности антивирусной компании ESET Лукас Стефанко. Он провел собственное исследование и выяснил, что пользователи гораздо чаще ошибаются и вводят учетные данные для доступа к своим счетам в фальшивых программах, чем попадают под действие вредоносных программ, ведущих самостоятельную деятельность (Украинский телекоммуникационный портал).

По словам Стефанко, исследователи в области информационной безопасности в своих отчетах незаслуженно списывают со счетов поддельные банковские приложения. Многие отраслевые эксперты не уделяют им должного внимания, полагая, что из-за своих ограниченных возможностей фальшивое банковское ПО не представляет опасности для большинства пользователей, которые уже научились отличать оригинал от подделки. Но это не так, констатирует Стефанко.

Поддельные банковские приложения для Android

Главное оружие поддельных банковских приложений, как ни странно, состоит в том, что они чаще всего полностью копируют легитимное ПО. Как правило, подделать страницу авторизации не представляет для мошенников особой сложности, а потому основной проблемой для них становится способ распространения таких программ. Но уж если пользователь доверился разработчику и скачал подделку на свое устройство, он с большой долей вероятности воспользуется им, отдав учетные данные злоумышленникам.

Поскольку Google смогла выработать весьма эффективную стратегию по блокированию поддельных приложений, пытающихся проникнуть в Google Play, чаще всего такое ПО, в том числе банковское, распространяется посредством сторонних источников и каталогов. Таким образом получается, что единственный, но надежный способ избежать обмана, – пользоваться только официальным магазином приложений от Google, который практически наверняка сможет обеспечить вашу безопасность и сохранность ваших сбережений.

(вгору)

Додаток 22

20.02.2019

В популярных менеджерах паролей обнаружилась очень опасная уязвимость

Эксперты по безопасности постоянно советуют людям использовать менеджеры паролей. Но, оказывается, сами эти менеджеры могут быть весьма небезопасными. Исследователи компании Independent Security Evaluators (ISE) обнаружили, что популярные решения содержат опасную уязвимость, которая может скомпрометировать абсолютно все пароли, сохраненные в менеджере (IGate).

Что конкретно произошло?

Команда ISE проанализировала приложения 1Password, Dashlane, KeePass и LastPass для Windows 10 и обнаружила, что самый главный мастер-пароль, открывающий доступ ко всем остальным, может сохраняться в оперативной памяти компьютера в формате обычного текста. Причем это происходит не только во время непосредственной работы с менеджером, но и тогда, когда тот находится в заблокированном виде в фоновом режиме.

Любой специалист, который сможет получить доступ к оперативной памяти ПК во время работы менеджера, сможет извлечь оттуда мастер-пароль. А дальше ему останется лишь воспользоваться этим главным ключом и слить всю базу ваших паролей подчистую.

Конечно, чтобы провернуть эту операцию, хакеру нужен доступ к оперативной памяти. Но это не обязательно должен быть физический доступ. Прочитать содержимое ОЗУ можно и удаленно, например, воспользовавшись соответствующим «троянским конем».

Что теперь делать?

Как ни странно, эксперты ISE не рекомендуют отказываться от использования менеджеров паролей. Как показывает практика, человек, который использует одинаковые или слишком простые пароли, находится в несоизмеримо большей опасности, чем тот, кто использует менеджер. Даже если этот менеджер уязвим.

Кроме того, теперь, когда о дыре стало известно, разработчики менеджеров постараются как можно быстрее выпустить обновления, которые исправят ситуацию. Потому – следите за обновлениями.

А до тех пор, пока уязвимость не устранена – просто выключайте менеджер, когда им не пользуетесь. Как уже говорилось выше, мастер-пароль от менеджера хранится в оперативной памяти ПК. Это происходит потому, что для удобства использования менеджеры рассчитаны на постоянную работу в фоновом режиме. Но если вы полностью закроете программу, данные из оперативной памятиу удалятся. А значит, правильная стратегия выглядит так: запустили менеджер паролей, воспользовались им, тут же его закрыли. Шанс на то, что кто-то украдет ваш мастер-пароль во время столь краткого использования, слишком мал, чтобы брать его во внимание.

(вгору)

Додаток 23

21.02.2019
Владимир Кондрашов

Украинскому видеоблогеру грозит два года тюрьмы за продажу вирусов

Украинцу, который вел в сети YouTube-канал о вирусах и продавал вредоносное программное обеспечение для кражи паролей, может грозить до двух лет тюрьмы. От внимания правоохранителей горе-видеоблогера не спасло ни использование запрещенных в Украине почтовых сервисов, ни переводы денег через снова-таки запрещенные платежные системы (InternetUA).

Об этом пишет InternetUA со ссылкой на определение Глуховского горрайонного суда Сумской области.

Как стало известно, работник Слобожанского управления киберполиции Департамента киберполиции Национальной полиции Украины получил информацию, что на форумах и в мессенджере Telegram неизвестный пользователь осуществляет сбыт вредоносных программ типа «Стиллер» и предлагает сотрудничество по распространению данного вредоносного программного обеспечения.

Для осуществления своей противоправной деятельности вышеуказанный пользователь использует мессенджер Telegram и программное обеспечение Skype, а также личные сообщения на форумах как средства связи, а в качестве оплаты за вредоносное ПО предлагает направить средства на запрещенный для обращения в Украине электронный кошелек Qiwi или банковскую карточку ПриватБанка.

При проверке информации установлено, что типом вредоносного ПО является Trojan, который путем скрытых программных процессов похищает пароли у потенциальной жертвы и формирует отчеты на почтовый адрес. Сбыт данного вредоносного программного обеспечения осуществляется под названием Build.exe.

Также установлено, что мужчина является автором и редактором канала YouTube, на котором рассказывается об использовании вредоносного программного обеспечения.

12 февраля дома у видеоблогера-продавца вирусов полицейские провели обыск. Суд своим определением наложил арест на изъятое имущество. За содеянное мужчине светит штраф от пятисот до тысячи необлагаемых минимумов доходов граждан или исправительные работы на срок до двух лет, или лишение свободы на тот же срок.

(вгору)

Додаток 24

20.02.2019

Microsoft заявила об атаках российских хакеров на организации Евросоюза

Microsoft обнаружила новые хакерские атаки на европейские аналитические центры и некоммерческие организации, которые занимаются

вопросами «демократии и прозрачности выборов» и «связаны с чиновниками». Об этом говорится в официальном блоге компании (InternetUA).

Ко многим из этих нападений, как уверены специалисты Microsoft по безопасности, были причастны хакеры из группировки под названием Strontium. Ее в корпорации ранее называли тесно связанной с российским правительством.

Атакам, по данным экспертов, в частности, подверглись сотрудники независимого немецкого объединения German Council on Foreign Relations (DGAP, Немецкое общество внешней политики), а также европейских отделений Института Аспена и Германского фонда Маршалла. Последняя организация представляет собой аналитический центр, который призван содействовать сотрудничеству и взаимопониманию между Северной Америкой и Европой.

Всего, как отметили в Microsoft, хакерским атакам подверглись 104 аккаунта, принадлежащих сотрудникам трех указанных организации. Нападения были нацелены на офисы в Бельгии, Франции, Германии, Польше, Румынии и Сербии. Атаки, согласно оценкам экспертов, совершались в период с сентября по декабрь прошлого года. Узнали специалисты о них недавно, говорится в блоге Microsoft.

Представители DGAP и европейских отделений Института Аспена и Германского фонда Маршалла были уведомлены об этом. Затем Microsoft, как уточнили в компании, предпринял ряд технических мер для защиты клиентов от этих атак.

Ранее о нападениях со стороны хакерской группировки Strontium Microsoft сообщала в августе прошлого года. После этого эксперты по кибербезопасности консалтинговой фирмы Accenture утверждали, что злоумышленники из Strontium также используют названия APT28, SNAKEMACKEREL и Fancy Bear. Последнюю группировку Минюст США в октябре 2018 года обвинил во взломе серверов Демократической партии в 2016 году и попытке взлома сетей Организации по запрещению химического оружия в 2018 году. Под названием Fancy Bear, по версии американских властей, скрывались сотрудники ГРУ (ныне Главное управление Генштаба Минобороны). Российские власти причастность к этим нападениям отрицают.

(вгору)

Додаток 25

21.02.2019

Баг в WhatsApp для iOS позволяет обойти защиту Touch ID и Face ID

Система биометрической защиты мессенджера WhatsApp для iOS содержит уязвимость, которая позволяет обойти ее любому желающему и получить доступ к переписке. Об этом сообщил пользователь Reddit с ником de_X_ter. По его словам, баг работает вне зависимости от выбранного способа идентификации, будь то Touch ID или Face ID, а взлом производится при

помощи штатного инструмента операционной системы под названием Share Sheets, предназначенного для обмена файлами (Украинский телекоммуникационный портал).

Взлом, по словам de_X_ter производится в считанные минуты. Чтобы операция удалась, необходимо проделать ряд простых действий.

Как взломать WhatsApp

- Для начала необходимо любым способом попасть в меню Share Sheets (русскоязычному пользователю этот инструмент известен под названием «Поделиться»). Это можно сделать, например, из приложения «Фото»;
- Далее следует выбрать WhatsApp в качестве способа обмена файлами;
- После того как вы это сделаете, вас перебросит в мессенджер, не потребовав прохождения верификации;
- Теперь необходимо свернуть приложение и выйти на рабочий стол, после его активировать его уже с рабочего стола. Если все манипуляции были выполнены верно, мессенджер не потребует от вас подтверждения личности.

Важно: данный метод обхода блокировки работает только при условии, если в настройках блокировки WhatsApp выбраны опции «через 1 минуту», «через 15 минут» или «через 1 час». При условии активации параметра «Немедленно», аналогичный трюк не сработает и вам не удастся обойти защиту мессенджера.

Обновление WhatsApp

Доподлинно неизвестно, осведомлены ли разработчики WhatsApp о существовании этой проблемы. Учитывая, что реализовать представленную выше инструкцию по обходу блокировки достаточно просто, эта проблема может повлечь за собой ряд негативных последствий и раскрытие конфиденциальной информации, разглашение которой абсолютно нежелательно.

(вгору)

Додаток 26

21.02.2019

Зарегистрировано широкое распространение Android-вирусов через Instagram

Производитель антивирусного программного обеспечения «Доктор Веб» сообщил о распространении Android-троянцев при помощи сервиса Instagram (InternetUA).

Речь идет о семействе вредоносных программ Android.HiddenAds, предназначенных для показа надоедливой рекламы. Вирусы постоянно отображают окна с баннерами и видеообъявлениями, которые перекрывают окна других программ и системный интерфейс, мешая нормальной работе с зараженными устройствами.

Поскольку троянцы показывают рекламу практически непрерывно, злоумышленники быстро окупают расходы на продвижение своих поделок через популярные интернет-сервисы.

С начала февраля 2019 года было выявлено почти 40 новых модификаций таких вредоносных приложений, их загрузили около 10 млн пользователей. Некоторые из этих троянцев мошенники распространяют через Instagram и YouTube.

Благодаря рекламе в популярных социальных сетях и интернет-сервисах с многомиллионной аудиторией число потенциальных жертв, которые могут установить опасные программы, значительно возрастает, предупреждают эксперты.

В течение февраля в компании «Доктор Веб» обнаружили в Google Play 39 новых модификаций троянцев семейства Android.HiddenAds. Они скрывались в полезных и безобидных программах: приложениях для фотосъемки, редакторах изображений и видео, сборниках обоев рабочего стола, системных утилитах, играх и другом ПО.

(вгору)

Додаток 27

22.02.2019

Браузер Firefox 67 будет предупреждать о скомпрометированных паролях и взломанных сайтах

В будущих версиях функции Firefox Monitor улучшатся методы безопасности. Как сообщается, эта функция была запущена в прошлом году и предназначалась для определения были ли учётные записи пользователей скомпрометированы. Теперь же, используя популярный сервис Have I Been Pwned, «Монитор» будет предупреждать о посещении небезопасных сайтов. В числе таковых будут ресурсы, которые ранее подвергались взлому. Таким образом, пользователь сможет узнать, были ли его учётные данные похищены (InternetUA).

Как ожидается, при попытке загрузить подобный ресурс будет выводиться соответствующее предупреждение. На данный момент функция уже доступна в ночных сборках Firefox и позволяет отслеживать небезопасные сайты. Разумеется, пока что пользователям приходится переходить на сайт Have I Been Pwned и вручную проверять безопасность своих аккаунтов и паролей, однако первый шаг уже сделан. В будущем проверка будет осуществляться прямо через Firefox Monitor.

Текущая версия позволяет либо проверить безопасность данных, либо отклонить уведомление. Во втором случае предупреждения больше не будут выводиться, а Firefox может предупреждать пользователя только в случае посещения сайтов, которые были скомпрометированы за последние 2 месяца. При этом сообщается, что первоначально тесты этой возможности приводились

ещё в Firefox 62, но теперь принято решение о переносе Firefox Monitor в основную кодовую базу 67-й версии браузера.

Подобное расширение есть и для Google Chrome. Оно называется Password Checkup и ищет любую информацию о компрометации пары логин-пароль. На данный момент сложно скачать, насколько такая функция улучшит безопасность, однако предполагается, что пользователи станут чуть внимательнее относиться к персональным данным и их сохранению.

(вгору)

Додаток 28

22.02.2019

Уязвимость WinRAR затронула полмиллиарда пользователей

WinRAR – один из самых скачиваемых архиваторов в истории, известный миллионам пользователей по всему миру. Но популярность софта нередко делает его мишенью для хакеров: как оказалось, под угрозой взлома оказались сотни миллионов обладателей копии знаменитого приложения (InternetUA).

Эксперты компании Checkpoint Research, работающей в сфере IT-безопасности, опубликовали отчёт о найденной уязвимости в коде архиватора WinRAR. По словам аналитиков, обнаруженный эксплойт позволяет злоумышленникам помещать вредоносный файл из состава архива формата ACE непосредственно в папку автозагрузки Windows, обходя при этом необходимость запуска приложения с повышенными привилегиями. «Слабым звеном» приложения оказалась библиотека UNACEV2.dll, не получавшая обновлений с 2005 года.

По данным портала ZDNet, поставщики эксплойтов уже проявили интерес к покупке уязвимостей в утилитах сжатия файлов в прошлом году, предлагая заплатить до 100000 долларов за инструмент удаленного выполнения кода в WinRAR, 7-Zip, WinZip (в Windows) или tar (в Linux). Аналитики утверждают, что в течение последних 19 лет риску заражения подверглось более 500 миллионов пользователей WinRAR.

Поскольку исходный код библиотеки оказался утерян, разработчики архиватора приняли решение отказаться от поддержки потенциально опасного формата и удалили соответствующие файлы в новой версии приложения. Пользователям WinRAR рекомендовано перейти на версию 5.70 beta 1, доступную для скачивания на официальном сайте.

(вгору)

Додаток 29

24.02.2019

Зараженные Android-приложения «съедают» до 10 ГБ мобильного трафика в месяц

Специалисты компании Oracle предупредили пользователей Android-устройств о новой вредоносной кампании, которая может обойтись им в кругленькую сумму в виде счетов за пользование мобильным интернетом (InternetUA).

Исследователи назвали кампанию DrainerBot и охарактеризовали ее как «крупнейшую мошенническую операцию с мобильными приложениями», и немудрено, ведь зараженные мошенниками приложения были загружены не менее 1 млн раз.

Специалисты Oracle обнаружили код DrainerBot внутри вредоносных SDK, связанных с Android-приложениями, в том числе с такими популярными, как Perfect365, VertexClub, Draw Clash of Clans, Touch ‘n’ Beat – Cinema и Solitaire: 4 Seasons (Full). Источником распространения вредоносных SDK является нидерландская компания Tapcore.

Когда жертва работает с зараженным приложением, DrainerBot незаметно запускает на ее устройстве скрытую рекламу, после чего приложение сообщает рекламной сети, будто ролик был просмотрен на легитимном сайте издателя, и мошенники получают денежное вознаграждение. Речь идет именно о видеороликах, так как они приносят наибольший доход.

Мошенническая кампания причиняет финансовый ущерб не только рекламщикам, но и пользователям зараженных приложений. Поскольку реклама запускается в фоновом режиме, жертва и не догадывается о расходе драгоценного мобильного трафика. По подсчетам исследователей, одно зараженное приложение способно «съедать» более 10 ГБ в месяц. Более того, реклама быстро истощает заряд аккумулятора, даже если вредоносное приложение не используется.

(вгору)

Додаток 30

26.02.2019

Facebook планировала следить за пользователями Android

Компания Facebook планировала использовать свое Android-приложение для отслеживания местоположения пользователей, а также разрешить рекламодателям отображать политическую рекламу и приглашать одиноких пользователей на сайты знакомств (InternetUA).

Как сообщают журналисты Computer Weekly, в руках у которых оказались внутренние конфиденциальные документы Facebook, компания работала над секретным проектом Growth Team по сбору данных владельцев Android-устройств. Инженеры разработали специальную технологию, позволяющую Android-версии приложения Facebook сопоставлять данные о местоположении пользователей с идентификаторами базовых станций с целью отображения контента, соответствующего этому местоположению.

О планах Facebook использовать данные пользователей Android сообщается в электронной переписке экс вице-президента по глобальной

политике компании Марни Линн Левин (Marne Lynn Levine) за 2012 год. «Мы будем собирать данные о местоположении пользователей и сопоставлять их с ID сотовых вышек. Эта информация будет храниться в анонимном виде, но позволит нам развертывать продукты в будущем», – сообщается в письме Левин.

По словам Левин, занимающей в настоящее время пост старшего операционного директора Instagram, Facebook изменила свои политики, для того чтобы рекламодателям было проще отображать рекламу сайтов знакомств одиноким пользователям. Изменения позволяли отображать рекламу не только пользователям, указавшим в профиле «без пары», но и тем, у кого семейное положение не указано вовсе. Как сообщается в письме Левин, подобное смягчение политики должно было увеличить прибыль компании от рекламы.

Согласно внутренним документам, Facebook также планировала собирать через свое Android-приложение данные о конкурирующих компаниях, в том числе узнавать, пользуется ли владелец устройства каким-либо другим магазином приложений помимо Google Play.

(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.