СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(13.03–26.03)

2019 № 6

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(13.03–26.03)
№ 6

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

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

14.03.2019
Ученые рассказали, чем соцсети вредны для здоровья

Мы проверяем соцсети, читаем новости, открываем почту сразу после отключения будильника. С одной стороны, это служит сигналом мозгу, что настало утро, пора просыпаться и включаться в работу. С другой – информация начинает поступать слишком резко.

Докладніше

***

14.03.2019
Как репосты в соцсетях влияют на поведение человека

Ежедневно в Facebook публикуют свыше четырех миллиардов сообщений, в Twitter – порядка пятисот миллионов. Причем больше половины – это репосты. Так люди делятся интересной, с их точки зрения, информацией. Почему одни сообщения распространяются с невероятной скоростью, а другие остаются практически незамеченными, как репосты влияют на поведение человека – читайте в нашем материале.

Докладніше

***

18.03.2019
Ирина Фоменко
The Guardian: зависимость от социальных сетей следует рассматривать как болезнь

Политики призвали к дальнейшему изучению влияния социальных сетей, но есть веские основания полагать, что такие сайты, как Facebook, Instagram и Twitter, которые постоянно конкурируют за то, чтобы пользователи проводили

больше времени на их платформах, могут иметь негативное воздействие на детей.

Докладніше

***

20.03.2019
С какого возраста ребенку можно иметь смартфон?

Решение о том, когда дать вашему ребенку его первый смартфон или планшет, гораздо важнее, чем может показаться на первый взгляд. С одной стороны, использование современных технологий – это всегда хорошо. С другой же слишком раннее формирование зависимости от гаджетов может отразиться на будущем ребенка. Однако зависимость от использования гаджетов – далеко не единственная проблема, которой стоит уделить внимание.

Докладніше

Маніпулятивні технології

12.03.2019
«Сапфір» розсилав українським військовим фейки та погрози

Створений російським генштабом спеціальний інформаційний підрозділ з кодовою назвою «Сапфір» здійснював розсилання листівок та СМС-повідомлень провокаційного змісту українським військовим. Про це під час брифінгу у Києві заявив начальник військової контррозвідки СБУ Сергій Левченко, передає кореспондент УНН (InternetUA).

За його словами, військова розвідка Російської Федерації поставила завдання щодо розсилання листівок, спрямованих на дискредитацію українських військових, як-то повідомлення зі звинуваченнями командування Збройних Сил України у нібито приховуванні бойових втрат.

«За задумом кураторів, це повинно було призвести до зниження морально-психологічного стану українських військових, що перебувають на лінії зіткнення, та їхнього залякування. Вказаною групою щоденно розсилалось понад 300 таких повідомлень», – сказав начальник військової контррозвідки СБУ.

Він зазначив, що поставлені російською розвідкою завдання «Сапфір» виконував за допомогою спеціально зареєстрованих у соцмережах сторінок про-українського і сепаратистського спрямування.

Загалом, зі слів Левченко, СБУ було виявлено понад 50 таких аккаунтів та 130 груп у соцмережах. Для розповсюдження фейкових повідомлень зловмисники також використовували спеціально розроблені сайти, задіювали месенджери та електронні поштові скриньки.

***

13.03.2019

Ольга Карпенко

В Facebook от имени банков предлагают 50 000 грн за ответы о любимых брендах. Это – мошенничество

На днях пользователи украинского Facebook могли столкнуться с разновидностью мошенничества, которое отличается не так оригинальностью идеи, как качеством исполнения.

Докладніше

***

14.03.2019

Мифы о вреде вакцинации распространяли в соцсетях из связанных с РФ аккаунтов, - Климкин

«Я вообще большой фанат того, что делает Ульяна Супрун и ее команда для вывода украинской системы здравоохранения из состояния глубокой комы.

А также мне очень импонирует, как госпожа министр построила коммуникацию с обществом и шаг за шагом развенчивает заскорузлые мифы о нашем здоровье. Вакцинация – это тема, которая годами обрастала именно такими предрассудками. К сожалению, мы видим, к чему это привело», – написал на своей странице в Facebook глава МИД Украины Павел Климкин (InternetUA).

Он подчеркнул, что большинство сообщений в соцсетях о вреде вакцинации были написаны из связанных с РФ аккаунтов: «Все, думаю, замечали, насколько российские тролли любят поживиться на теме вакцинации. Исследователи проанализировали тысячи сообщений в соцсетях, которые распространяли антивакцинаторские мифы: большинство из них, как и в случае с вмешательством в американские выборы, были написаны из связанных с Россией аккаунтов. Именно так подрывают общественное доверие к усилиям системы здравоохранения для повышения уровня вакцинации населения в Украине и во всем мире. А потом, посеяв раздор и общественные волнения, Россия использует критическую эпидемиологическую ситуацию как аргумент в своих failed state упреках к Украине и других странах».

«Эта дезинформационная кампания против здоровья во всем мире – неотъемлемая составляющая гибридной войны России против человечества», – сообщил он, добавив, что делая прививки, граждане усиливают иммунную систему онлайн-дискурса и нейтрализуют российский дезинформационный вирус.

***

25.03.2019

Інформаційна атака на прикордонників: невідомі лякають «третім Майданом» і спецназом США

Українські прикордонники отримують повідомлення від невідомих адресантів з попередженнями про «Майдан 3.0» та спецназівців США, які прилетіли в Україну, щоб стабілізувати ситуацію на період «невизначеності» та віддати владу міністру внутрішніх справ Арсену Авакову (InternetUA).

Про це написав у Facebook речник Державної прикордонної служби Олег Слободян.

За словами Слободяна, в повідомленнях йдеться про, нібито, таємне прибуття до Києва «американського спецназу», що питання «Майдану 3.0» вже вирішено і не має сенсу служити бо «за вас все уже порешали».

«Державна прикордонна служба офіційно заявляє, що жоден американський, чи будь-який інший спецназ в Україну не прибував», – повідомив речник ДПСУ.

Слободян закликав не піддаватися на провокації й додав, що джерела цих «повідомлень» будуть встановлені досить швидко.

«Якщо подібні СМС приходять і вам на телефон – повідомляйте в компетентні правоохоронні органи», – написав він.

Спецслужби і технології «соціального контролю»

13.03.2019
Facebook удалила рекламу кандидата в президенты США

Facebook удалила несколько рекламных объявлений кандидата в президенты США, сенатора от демократической партии Элизабет Уоррен. Об этом сообщает Politico (InternetUA).

По данным издания, соцсеть удалила рекламу Уоррен, в которой она призывала к распаду Facebook и других технологических гигантов.

Как отмечается, компания объяснила удаление объявлений нарушением политики социальной сети.

При этом в последствии Facebook решила восстановить рекламные посты Уоррен для разрешения «активных дискуссий».

***

16.03.2019
Facebook вводит инструменты для борьбы с «порноместью»

Facebook анонсировал новую систему на базе ИИ, которая предназначена для удаления чужих фотографий в стиле «ню». Facebook начал борьбу с порноместью еще в конце прошлого года. Уже тогда они разработали систему по нахождению и удалению подобных материалов. Но на том этапе, чтобы

обезопасить пользователей, им предлагалось выслать собственные фотографии, которые затем использовались для блокировки подобных изображений (InternetUA).

По словам представителей социальной сети, новая система на базе ИИ способна самостоятельно выявлять обнаженные фотографии. Затем программа отправляет их модератору, который и решает, нужно ли блокировать фото или видео или нет.

«Используя машинное обучение и искусственный интеллект, мы теперь можем быстро обнаруживать изображения или видео с обнаженными людьми, которые публикуются без разрешения в Facebook и Instagram. Это означает, что мы можем найти этот контент до того, как кто-либо сообщит о нем. Это важно, так как что зачастую жертвы боятся возмездия и не хотят сами сообщать о контенте, или они не знают о том, что контент был опубликован», – пишут представители Facebook.

Facebook также создал новую страницу в своем Центре безопасности, где рассказывается, какие шаги следует предпринять жертвам порномести.

***

17.03.2019
Ирина Фоменко
Почему Facebook не отключил трансляцию резни в Новой Зеландии

Преступник использовал Facebook, чтобы транслировать в прямом эфире убийство десятков людей в Новой Зеландии. Но независимо от того, как Facebook – и Twitter, и YouTube, и Reddit, и другие платформы, помогшие распространять изображения и видео с массовой стрельбы в Крайстчерче, которую власти сочли террористической атакой – отвечают на критику в отношении их ролей сегодня, нужно помнить ключевую вещь о платформах – они сделали именно то, для чего они предназначены: позволили людям делиться тем, что они хотят, когда они хотят, с таким количеством пользователей, как они хотят.

Докладніше

***

19.03.2019
Facebook посилює боротьбу з фейками перед виборами до Європарламенту

Facebook посилює правила із запобігання поширенню неправдивих новин перед виборами до Європарламенту, які заплановані на 26 травня (Espreso.tv).

Про це повідомила одна з топ-менеджерів компанії Тесса Лайонс, передає DW.

Зокрема, Facebook планує створити новий віртуальний ситуаційний центр, куди будуть підключатися співробітники соцмережі з різних офісів.

За словами Лайонс, Facebook по всьому світу працює з питання неправдивих (фейкових) новин із 43 організаціями. А передвиборний ситуаційний центр стане готовою схемою для майбутнього вирішення проблем з поширенням фейкових новин у Facebook.

Соцмережа також планує організувати цілодобову співпрацю розробників програм, спеціалістів з обробки даних і політичних експертів.

Співробітники такого центру зможуть зв'язуватися з різними відомствами, зокрема й у Німеччині, де одним із адресатів стане Федеральне відомство з безпеки у сфері інформаційних технологій.

Лайонс сказала, що ситуаційний центр здійснюватиме свою діяльність у кількох місцях, зокрема, у штаб-квартирі Facebook в Каліфорнії і головному європейському офісі в Дубліні.

Представниця Facebook повідомила, що кількість людей, зайнятих у боротьбі з фейковими новинами, збільшиться з 20 тис. до 30 тис.

Планується, що нова структура Facebook продовжить роботу і після виборів в Євросоюзі.

***

18.03.2019

Доказом вини прокурора стало листування у месенджері

Посадовця звільнили через вимагання неправомірної вигоди та розголошення відомостей досудового розслідування особі, причетній до злочину.

Докладніше

***

19.03.2019

В Чехії працювала група російських хакерів

Про це у власному розслідуванні про створення російськими спецслужбами двох комп’ютерних фірм у Празі пише чеське видання Respekt (InternetUA).

За даними журналу, формально ці компанії займалися продажами комп'ютерного обладнання та програмного забезпечення. Утім, їх співробітники також готували хакерські атаки, а частину техніки для цих фірм в Чехію привозили з Росії на автомобілях російського посольства з дипломатичними номерами.

Група могла співпрацювати з кількома аналогічними російськими осередками в інших країнах. Група кіберзловмисників нібито включала як чехів, так і росіян з місцевим громадянством.

Чеські правоохоронці розкрили діяльність угрупування ще на початку 2018 року та провели низку затримань. Утім, підсумки і деталі цієї операції досі не розголошувалися.

***

20.03.2019

Сенат США требует объяснений от IT-компаний из-за трагедии в Новой Зеландии

Руководителей Facebook, YouTube, Google и Microsoft вызывают в Сенат на экстренный брифинг – дело в том, что Комитет по внутренней безопасности заинтересовался ситуацией с распространением видео, на котором террорист расстреливает прихожан в мечети новозеландского города Крайстчерч. Онлайн-платформы не смогли вовремя заблокировать жестокий ролик, из-за чего он мгновенно разошелся по интернету.

Докладніше

***

20.03.2019

Петр Порошенко продлил блокировку Яндекса до марта 2022 года

Президент Украины Петр Порошенко ввел в действие санкции Совета национальной безопасности и обороны против причастных к российской агрессии против Украины. Об этом свидетельствует указ президента №82/2019, сообщает «ЛІГА.net» (InternetUA).

Всего, по инициативе Кабмина, СБУ и НБУ в санкционный список попали 294 юридических и 848 физических лиц.

В частности, на последующие три года санкции, в виде блокирования активов, ограничения торговых операций, запрета провайдерам предоставлять доступ пользователям и другие ограничения, были введены по отношению к компании Яндекс и всех ее сервисов (Яндекс Такси, Яндекс Карты, Яндекс музыка и других).

Примечательно, что двух других крупных российских ИТ-компаний – VK и Mail.Ru, которые вместе с Яндекс попали под санкции в мае 2017 года, в списке нет. Это означает, что если санкции не продлят, то для деятельности в Украине VK и Mail.Ru после мая 2020 года не будет никаких ограничений.

***

21.03.2019

СБУ фіксує активізацію втручання спецслужб РФ у виборчі процеси в Україні

Служба безпеки України у ході виконання покладених на неї завдань із забезпечення інформаційної безпеки держави фіксує активізацію спецслужб РФ

із втручання у виборчі процеси в Україні через використання соціальних мереж для маніпулятивного впливу на електоральні настрої українських користувачів мережі Інтернет.

Докладніше

***

22.03.2019

СБУ викрила чотирьох проросійських інтернет-агітаторів

У Миколаєві затримали чотирьох чоловіків, що займалися антиукраїнською пропагандою (InternetUA). Про це йдеться у повідомленні прес-служби Служби безпеки України.

Чоловіки поширювали у мережі Інтернет матеріали, спрямовані на штучне загострення суспільно-політичної ситуації напередодні виборів. Вони «працювали» у соцмережах «ВКонтакте» та Facebook через публічні групи.

До їх угрупування також входило ще четверо одеситів. Учасники мережі отримували винагороду за поширення закликів до зміни меж державного кордону України через сервіси грошових переказів.

***

25.03.2019

WhatsApp получил новую функцию для блокировки чужих аккаунтов

Как стало известно, данный мессенджер в последней бета-версии получил важнейшую новую функцию, а обернуться она может тем, что чужую учетную запись заблокируют.

Докладніше

Проблема захисту даних. DDOS та вірусні атаки

13.03.2019

Соцмережа Facebook пояснила у Twitter причину масштабного збою

Адміністрація соцмережі Facebook заявляє, що глобальний технічний збій у Facebook та Instagram міг статися через DDoS-атаку. Про це йдеться у заяві Facebook, оприлюдненій у Twitter (InternetUA).

«Ми знаємо, що сьогодні у багатьох користувачів виникли проблеми із доступом до сімейства додатків Facebook. Ми намагаємося вирішити проблему якнайшвидше. Не можемо підтвердити, що проблема не пов'язана зDDoS-аткою», – йдеться у повідомленні соцмережі.

Нагадаємо, 13 березня у роботі Facebook і Instagram стався збій серед користувачів Західної Європи, а також США. За даними сервісу, постраждали, зокрема, користувачі даних соцмереж з України, Росії та Білорусі.

Як повідомляли користувачі, в обох соцмережах пропала можливість публікувати записи, а також відправляти і отримувати повідомлення.

***

13.03.2019

В Facebook невозможно отключить поиск профиля по номеру телефона

Пользователи соцсети недовольны тем, что телефонные номера, которые Facebook требует вводить при прохождении двухфакторной аутентификации, привязываются к их профилям: в результате кто угодно может найти пользователей по их номеру.

Докладніше

***

13.03.2019

Bloomberg: хакеров из России заподозрили в атаке на выборы в Индонезии

Российские и китайские хакеры атакуют базу данных избирателей Индонезии с целью сорвать предстоящие президентские выборы в стране, пишет агентство Bloomberg со ссылкой на главу индонезийской избирательной комиссии Арифа Будимана (InternetUA).

Во время подготовки к выборам в Индонезии, которые пройдут 17 апреля, государство столкнулось с волной кибератак. По словам Будимана, следы некоторых из атак ведут в Россию и Китай. Кибероперации включали попытки «манипулировать или изменять» контент, а также создание фейковых избирателей.

По словам Будимана, избирательную систему пытаются взломать «не только каждый день, но почти каждый час». Однако он не прояснил, является ли целью кибератак поддержка определенного кандидата. Индонезия не предоставила дополнительной информации об обвинениях, говорится в материале.

Отмечается, что власти Индонезии начали расследование по обвинению в мошенничестве на предстоящих выборах. При наличии доказательств хакерского вмешательства Китай выразил готовность оказать содействие в расследовании властей Индонезии, пишет агентство.

***

13.03.2019

Киберпреступники атакуют интернет-магазины на базе WordPress

Злоумышленники атакуют интернет-магазины на базе WordPress с помощью бэкдора, которым они заражают сайты через уязвимость в плагине Abandoned Cart Lite for WooCommerce.

Докладніше

***

14.03.2019

США розслідують «злив» компанією Facebook даних сотень мільйонів користувачів, – NYT

Виробники смартфонів й інших пристроїв підписали угоду із Facebook і при цьому отримали доступ до персональних даних сотень мільйонів користувачів соцмережі (Espreso.tv).

Суд у Нью-Йорку вимагає документи хоча би від двох відомих виробників смартфонів чи інших пристроїв.

Серед цих компаній було понад 150, в тому числі Amazon, Apple, Microsoft і Sony, які уклали угоди із Facebook, які дозволяють компаніям бачити друзів користувачів, контактну інформацію та інші дані, іноді без згоди власне користувачів.

«Ми співпрацюємо зі слідчими і серйозно ставимося до цих розслідувань. Ми надали публічні свідчення, відповіли на питання і пообіцяли, що будемо продовжувати робити це», – йдеться в заяві представника Facebook.

Зазначається, що за останні два роки Facebook припинив більшість партнерських відносин.

***

14.03.2019

Владимир Кондрашов

ИнАУ: в UA-IX запускается услуга противодействия DDoS-атакам

ДП «Украинская сеть обмена трафиком UA-IX» в партнерстве с ООО «Хайлоад Системс» запускает услугу противодействия DDoS-атакам (InternetUA).

Как стало известно, услуга будет предоставляться ООО «Хайлоад Системс» Участникам UA-IX с использованием внедренной в декабре 2018 автоматизированной системы управления VLAN.

По словам исполнительного директора Интернет Ассоциации Украины Владимира Куковского, сеть обмена трафиком никак не зарабатывает на данном предложении.

– Защита лишней не бывает. Такую услугу на украинском рынке на самом деле предлагают много компаний. «Хайлоад Системс», по мнению Правления ИнАУ, предложила конкурентные цены для участников UA-IX. Мы предоставили порт этой компании в 40 Гбит/с. При этом сама сеть обмена

трафиком UA-IX на этом никак не зарабатывает. Здесь нет её коммерческого интереса. Он в другом: во-первых, наши члены получат дополнительную возможность защиты от DDoS-атак прямо через сеть обмена трафиком. Во-вторых, у нас запущен проект автоматических VLAN-ов, и мы рассчитываем на рост числа их заказов, – объясняет Владимир Куковский.

Для участников UA-IX операторов/провайдеров предусмотрено несколько уровней услуги:

***

14.03.2019
Владимир Кондрашов
Эксперты: хакеры проводят «разведку боем» от имени НАПК

13 марта была осуществлена массовая рассылка вредоносных документов (MS Word Document), «вооруженных» макросом. Атака была направлена на украинские органы государственной власти и финансовые учреждения.

Докладніше

***

14.03.2019
Найден единственный способ отличить фальшивую регистрацию через аккаунт в Facebook от настоящей

На различных сомнительных сайтах пользователям выводятся всплывающие окна с предложением зарегистрироваться через Facebook. Эти окна неотличимы от настоящих, но на деле только крадут логины и пароли.

Докладніше

***

15.03.2019
Уязвимость нулевого дня в Windows позволяет получить контроль над ПК жертвы

Специалисты «Лаборатории Касперского» обнаружили в Windows ранее неизвестную уязвимость, которая, предположительно, использовалась для проведения целевых атак по крайней мере двумя кибергруппировками – FruityArmor и недавно обнаруженной SandCat. Сведения о бреши, получившей номер CVE-2019-0797, были переданы в Microsoft; соответствующий патч уже выпущен (Компьютерное Обозрение).

Данная уязвимость позволяет злоумышленникам получить доступ к сети или устройству жертвы. Для ее использования был написан эксплойт, нацеленный на 8 и 10 версии Windows. Брешь в графической подсистеме для расширения локальных привилегий позволяет киберпреступникам получать полный контроль над атакуемым компьютером

***

15.03.2019

Две трети антивирусов в Google Play Store оказались ненастоящими

Австрийская организация AV-Comparatives, занимающаяся тестированием антивирусных продуктов, опубликовала отчёт об исследовании, показавшем, что две трети антивирусов для платформы Android выполняют свою работу некачественно или не делают вообще ничего.

Докладніше

***

17.03.2019

В терминалах оплаты нашли ворующий деньги вирус

Опасный вирус DMSniff атаковал терминалы оплаты и крал данные банковских карт. Вредоносную программу обнаружили сотрудники компании Flashpoint, их исследование опубликовано на портале BleepingComputer (InternetUA).

Вирус попадает в устройство либо путем подбора пароля, либо через эксплуатацию уязвимостей. В ходе мониторинга зараженного устройства программа ищет данные о банковских картах и передает их в руки злоумышленников.

Вредоносное ПО также скрывает передаваемые данные, чтобы зашифровать свои действия. Жертвами хакеров чаще всего становились развлекательные предприятия и кафе.

Преступники используют DMSniff с 2016 года. С тех пор исследователи в области кибербезопасности обнаружили более десятка различных вариаций вируса.

В прошлом году преступники из группировки JokerStash (известна также как Fin7) украли платежные данные пяти миллионов американцев. Информация о 125 тысячах из них была сразу выставлена на продажу. Жертвы были постоянными покупателями магазинов Lord & Taylor и Saks Fifth Avenue.

***

17.03.2019

Російські хакери активізують роботу перед виборами в Україні, – кіберполіція

В українському кіберпросторі починають проявляти активність хакерські групи, що мають стосунок до РФ, на кшталт Fancy Bear, The Shadow Brokers та інші. Напередодні виборів вони намагаються отримати доступ до мереж державних органів (InternetUA).

Про це заявив керівник кіберполіції Сергій Демедюк.

«Останнім часом зазнають системних атак усі центральні органи виконавчої влади, зокрема й ті, що перебувають під захистом Держспецзв'язку. Мета – проникнути в їхню мережу. Однак успішних атак ми не виявили», – наголосив Демедюк.

Він також повідомив, що вже були зафіксовані спроби «протестувати» атаками сайт ЦВК.

Нещодавно фахівці відомства допомагали усунути атаки Міністерству агрополітики та Мін'юсту, уточнив Сергій Демедюк.

За словами очільника відомства, часто працівники кіберполіції усувають хакерські атаки на українські суди.

Все частіше поліцейські фіксують масові поширення модифікованого шкідливого програмного забезпечення, яке зловмисники РФ вже використовували під час атак на об'єкти критичної інфраструктури, а також нового, з яким раніше українські фахівці не стикалися.

***

18.03.2019

Манипуляции с DNS и целенаправленные атаки будут наиболее опасными для предприятий

Несмотря на то, что к некоторым видам атак хакеры обращаются из года в год (фишинг и инъекции SQL-кода), в прошлом году злоумышленники начали применять новые методы, рассказали на конференции RSA эксперты SANS Institute. Они выделили пять самых опасных методов атак, с которыми предприятия могут столкнуться в этом году.

Докладніше

***

18.03.2019

Мошенники используют крушение Boeing в Эфиопии для распространения вредоносного ПО

Спамеры стараются не упустить ни единой возможности воспользоваться ажиотажем вокруг громких событий с целью привлечь внимание интернет-пользователей. Последние несколько дней одними из самых обсуждаемых событий в мире являются теракт в Новой Зеландии и крушение самолета Boeing 737 Max в Эфиопии. Кибермошенники не преминули воспользоваться всеобщим вниманием к этим событиям и развернули новую вредоносную кампанию (InternetUA).

Согласно сообщению специалистов из 360 Threat Intelligence Center, злоумышленники используют крушение самолета для распространения вредоносного ПО. Мошенники рассылают спам с предположительно взломанной электронной почты @IsgecPresses (info@isgec.com) и помечают его

хэштегом #Boeing. В теме писем, как правило, указано: «Fwd: Airlines plane crash Boeing 737 Max 8».

Вредоносные письма замаскированы под пресс-релиз от частного аналитика, якобы обнаружившего некие документы в даркнете. В этих документах будто-бы указан список авиакомпаний, чьи самолеты в ближайшем будущем ждет такое же крушение.

Письма содержат вложение в виде файла JAR (MP4_142019.jar), играющего роль дроппера вредоносного ПО Houdini H-WORM. Когда жертва его открывает, файл сразу же выполняется на системе компонентом JAVA. Изначально исследователи полагали, что файл устанавливал только Houdini H-WORM, однако это оказалось не так. Как сообщили специалисты из Racco42, он также устанавливает на компьютер жертвы инфостилер Adwind.

Министерство внутренней безопасности США также предупредило пользователей соблюдать осторожность в связи с возможным использованием спамерами теракта в Новой Зеландии.

***

18.03.2019

Число утечек данных из медицинских учреждений выросло на 16 % за год

Компания InfoWatch представила свои данные по утечкам конфиденциальной информации из учреждений здравоохранения в прошлом году. Аналитический центр компании зарегистрировал 429 утечек из различных учреждений медицинской сферы по всему миру за год.

Докладніше

***

18.03.2019

DARPA работает над абсолютно защищенной системой голосования

Министерство обороны США потратит $10 млн на разработку инновационной технологии проведения выборов. Следить за ходом голосования смогут избиратели, а взломать систему будет невозможно: проверять надежность ПО и «железа» будут хакеры со всего мира.

Докладніше

***

18.03.2019

Владимир Кондрашов

Укрпочта засветила в сети конфиденциальные данные

Эксперт по кибербезопасности Александр Галущенко обнаружил в свободном доступе в сети несколько терабайт данных «Укрпочты», среди

которых – списки клиентов и почтовых отправлений, финансовая информация компании и другие конфиденциальные данные. По подсчетам эксперта, «дыра» в безопасности, в случае её использования злоумышленниками, могла стоить национальному почтовому оператору полмиллиарда гривен.

Докладніше

***

19.03.2019
Ирина Фоменко
ЕС принял новый протокол реагирования на крупные кибератаки

Европол 18 марта объявил о принятии нового протокола о том, как правоохранительные органы в Европейском Союзе и за его пределами будут реагировать на крупные трансграничные кибератаки.

Докладніше

***

19.03.2019
ЄС виділив 525 млн євро на військові дослідження, з них 182 млн – на боротьбу з кіберзагрозами

Єврокомісія ухвалила пропозиції щодо фінансування оборонних проектів на суму 525 млн євро протягом 2019-2020 років (Espreso.tv). Про це повідомляє прес-служба Європейської Комісії.

«Співпраця в сфері оборони є єдиним шляхом для того, щоб захистити європейців у цьому нестабільному світі. Ми робимо нашу частину. Спільні проекти вже матеріалізуються. Європейська оборона відбувається», – заявив віце-президент Єврокомісії Юркі Катайнен.

Зазначається, що в організації створюють Фонд європейської оборони до 2021 року. Йдеться про фінансування проектів, пов’язаних із сучасними технологіями та інноваціями в таких сферах як штучний інтелект, технологія безпілотних апаратів, супутниковий зв’язок та розвідувальні системи.

Єврокомісія оприлюднила інформацію, на які саме програми виділено фінансування.

80 млн євро передбачено на забезпечення боєздатності, захисту й мобільності військ за рахунок створення супутникових систем виявлення загроз та боротьби з безпілотниками, 182 млн євро -–на розвідку, захищений зв'язок та боротьбу з кіберзагрозами. Ще 71 млн євро буде витрачено на розвиток ударних систем наземного, повітряного та морського базування, йдеться у повідомленні.

Наголошується, що окреме фінансування передбачене для так званих інноваційних оборонних технологій – 27 млн євро спрямують на розвиток штучного інтелекту, віртуальної реальності та кібернетичних технологій.

Ще 100 млн євро передбачається витратити на розвиток програми «Євродрон», яка є важливою для забезпечення стратегічної автономії Європи. 37 млн євро спрямовуються на розвиток взаємосумісності та надійності військового зв'язку, зазначають у Єврокомісії.

***

20.03.2019

Мощное интернет-оружие усилилось и атаковало новые устройства

В сети обнаружен новый вариант опасного вируса Mirai. В него входит 27 программ-эксплоитов, использующих уязвимости в защите. О находке сообщили сотрудники компании Palo Alto Networks (InternetUA).

Новыми целями стали коммерческие устройства интернета вещей – телевизоры и устройства для работы с презентациями. Помимо них, Mirai по-прежнему атакует серверы, роутеры и умные гаджеты.

Ранее вирус использовал для взлома в основном метод подбора логина и пароля. Список таких данных, автоматически применяемый к атакуемым устройствам, был расширен. Помимо этого, почти половина из обнаруженных эксплоитов ранее не встречалась в арсенале злоумышленников.

Сообщается, что новые возможности дают ботнету большую поверхность для атаки. В частности, взлом корпоративных сетей может увеличить пропускную способность для DDoS-атак. Это автоматически усилит ботнет.

В конце октября 2018 года стало известно, что один из создателей Mirai по имени Парас Джа (Paras Jha) был приговорен к шести месяцам домашнего ареста и штрафу в 8,6 миллиона долларов. Министерство юстиции США сообщило, что он был признан виновным в запуске DDoS-атак.

***

21.03.2019

Уязвимость в Android: хакеры могли получить доступ к любому смартфону

Специалисты компании Positive Technologies обнаружили критическую уязвимость в браузере Google Chromium, которая позволяла получить доступ к личным данным пользователей. Сотрудник этой организации Сергей Тошин нашел баг еще в декабре прошлого года, после чего сообщил Google о такой проблеме (InternetUA).

Как стало известно, несколько недель назад технологический гигант исправил ошибку. А в новом исследовании Positive Technologies подробнее рассказано об уязвимости.

Так, в отчете организации говорится, что проблема связана с компонентом Android WebView, который используется для отображения страниц в Android-приложениях. Как оказалось, уязвимость была в движке

Chromium и затронула все версии мобильной системы, начиная от Android 4.4 и выше.

Хакеры могли воспользоваться данной уязвимостью, чтобы заразить устройства пользователей вредоносными приложениями с помощью службы Instant Apps. Данные программы получают доступ к аппаратному обеспечению смартфона и перехватывают пользовательские данные.

Владельцы устройств на базе Android 7.0 и выше должны были получить обновление браузера Google Chrome с соответствующими исправлениями еще в январе. Пользователи более ранних версий Android пришлось обновлять WebView самостоятельно через сервис Google Play.

***

21.03.2019

Найден способ взломать сайты через PDF-файлы

Анонимный хакер, скрывающийся под псевдонимом Polict, обнаружил в генераторе PDF-файлов TCPDF опасную уязвимость. В своем блоге он описал, как злоумышленники могут взломать сайты, воспользовавшись этой брешью (InternetUA).

Библиотека TCPDF используется множеством сайтов: с ее помощью код HTML можно преобразовать в PDF-документ. Для того чтобы воспользоваться уязвимостью, киберпреступники должны либо вмешаться в процесс генерации, либо самостоятельно встроить в HTML вредоносный код.

Ошибка получила код CVE-2018-17057. Использовать брешь в атаке достаточно сложно, однако в случае успеха хакеры получают полный контроль над скомпрометированным сайтом.

Белый хакер Polict обнаружил проблему в TCPDF еще летом 2018 года и сообщил о находке сотрудникам компании-производителя. Для устранения ошибки им пришлось дважды обновлять свой продукт.

***

21.03.2019

Крупные европейские сайты бастуют против принятия скандальной «Директивы о копирайте»

О скандальной «Директиве о копирайте» мы уже писали не раз. В последний раз мы вспоминали о ней, когда оказалось, что надежды на разумное решение Европарламента были напрасны (InternetUA).

Тогда же мы сообщали, что документу ещё предстоит пройти заключительный этап голосования Европарламента, который пройдёт когда-то в промежутке между 25 марта и 18 апреля. Точнее, если верить свежим данным, это произойдёт уже 26 марта.

И вот 21 марта ряд крупных онлайн-ресурсов решил в очередной раз поднять вопрос спорного документа.

К примеру, ряд европейских доменов «Википедии» на данный момент не работает, выводя вместо главной страницы обращение к пользователям с просьбой подписать петицию против введения тех самых спорных статей директивы.

К протесту присоединились и другие сайты. В частности, Twitch, PornHub и Reddit, но последний силами непосредственно пользователей.

Говоря об упомянутой петиции, её уже подписали более 5 млн человек.

***

21.03.2019

Google добавит в Chrome защиту от слежки со стороны сайтов

Компания Google продолжает совершенствовать методы безопасности для своего браузера. Ведь на сегодняшний день есть множество способов шпионить за пользователями, используя веб-сайты, которые обращаются к определённым API-интерфейсам. Одним из способов, который появился несколько лет назад, стал анализ данных акселерометра смартфона.

Докладніше

***

21.03.2019

Ирина Фоменко

Уязвимость в Google Фото позволяет преступникам узнать местоположение жертвы

Через браузерные тайминг-атаки хакеры могут анализировать данные изображения, чтобы узнать, когда человек посещал определенное место. Это не обычная угроза, и она наиболее эффективна в целевом сценарии, но вредоносный веб-сайт можно использовать и для доступа к фотографиям.

Докладніше

***

22.03.2019

«Укртелеком» усиливает защиту своей инфраструктуры на период выборов

По сообщению оператора, был повышен уровень защиты его телекоммуникационной сети на период выборов. В частности, проведена инспекция кабельных линий вдоль автотрасс, обеспечена усиленная частная охрана отдельных участков и физическое блокирование доступа к кабельной канализации, делает невозможным проникновение в колодец (Компьютерное Обозрение).

В свою очередь силовые структуры также уделяют особое внимание недопущению краж и повреждений телекоммуникационных кабелей. Перечень

ключевых участков сети передан министерстру внутренних дел Арсену Авакову во время координационного совещания с участием руководителей Службы безопасности Украины, Центральной избирательной комиссии, Национальной полиции и представителей Госспецсвязи и киберполиции.

***

22.03.2019

Facebook устранила неполадку, открывшую миллионы паролей

21 марта Facebook сделала официальное заявление о том, что устранила проблему, в результате которой пароли миллионов пользователей социальной сети оказались видны служащим этой компании (Компьютерное Обозрение).

По оценкам исследователя Брайана Кребса (Brian Krebs), автора блога по вопросам кибербезопасности, KrebsOnSecurity, к паролям в открытом для чтения формате могли иметь доступ до 20 тысяч служащих компании.

«Эти пароли никогда не были видны никому за пределами Facebook, и на сегодняшний день мы не нашли никаких доказательств того, что кто-нибудь внутри компании незаконно просматривал или использовал их», – заявила компания.

KrebsOnSecurity, ссылаясь на одного из старших сотрудников Facebook, пишет, что по данным внутреннего расследования в текстовом формате хранились пароли учётных записей от 200 до 600 млн пользователей Facebook. Самые ранние из них могли датироваться 2012 годом.

По сообщению самой компании, недоработка защиты вскрылась в январе в ходе плановой проверки безопасности. Большинство затронутых инцидентом подписчиков являются пользователями Facebook Lite, версии приложения для районов с плохим подключением к Интернету.

«По нашим оценкам, нам предстоит уведомить сотни миллионов пользователей Facebook Lite, десятки миллионов других пользователей Facebook и десятки тысяч пользователей Instagram», – сказали в компании.

***

26.03.2019

5 лучших антивирусов на Android

Вредоносное ПО для Android является серьезной проблемой для пользователей самой популярной в мире мобильной операционной системы. Представляем вам пять лучших антивирусных приложений для Android-устройств.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

13.03.2019

У соцмережах вірусний хештег #Trashtag: По всьому світу люди прибирають парки і пляжі

Флешмоб під назвою Trashtag Challenge закликає людей влаштовувати прибирання в різноманітних місцях, і тисячі інтернет-користувачів вже так і роблять (InternetUA).

Механізм такий: потрібно сфотографувати будь-яке місце, що перебуває в занедбаному стані, прибрати його, а потім викласти два фото – до і після прибирання.

У соцмережах вже можна знайти чимало знімків прибраних пляжів і парків. Учасники флешмобу сподіваються, що надалі його популярність тільки зростатиме.

***

16.03.2019

Чат-боты в Viber и Telegram оповестят украинцев об изготовлении ID-карт и загранпаспортов

Государственная миграционная служба Украины (ГМС) ввела новый сервис, с помощью можно проконсультироваться по оформлению биометрических документов и пользоваться официальными электронными сервисами миграционной службы в интерактивном режиме (InternetUA).

В помощь этому будут чат-боты для мессенджеров Viber и Telegram.

Они зададут вопросы о личных условиях оформления документа и сообщат, что именно нужно иметь с собой во время оформления в миграционной службе или центре предоставления административных услуг.

Кроме того, помощью ботов можно получить консультацию об оформлении всех биометрических документов, которые выдает ГМС: ID-карт, заграничных паспортов, а также вида на постоянное и временное проживание для иностранцев и лиц без гражданства.

Помимо помощи в оформлении, заказчик может также получать в мессенджере сообщения о каждом новом этапе оформления документа вплоть до момента, когда документ прибудет в подразделение для выдачи.

***

14.03.2019

Украинская организация запустила чат-бот, который поможет отсортировать мусор

Организация «Україна без сміття» запустила чат-бот в Telegram, который поможет пользователям научиться сортировать мусор, отмечает the-village.com.ua (Marketing Media Review).

В чат-боте также содержится информация о месте и график работы станций, где принимают вторсырье. Программа имеет функции подсказок, поиска, переадресовывает пользователя на соответствующую страницу.

***

21.03.2019

Флешмоб LotsOfSocks: на знак підтримки людей із синдромом Дауна учасники вдягають різні шкарпетки

Різнокольорові шкарпетки – як символ зайвої хромосоми і спосіб відчути себе не такими як усі інші, як «люди сонця», які завжди знаходяться під пильним і часто недобрим поглядом оточуючих (Espreso.tv).

Фото із хештегом #LotsOfSocks користувачі публікують у Facebook та Twitter.

Зазначається, що у світі із синдромом Дауна народжується кожна 700 дитина, а в Україні зараз живе близько 19 тисяч таких людей

До акції долучились й українські політики. Зокрема, Роман Безсмертний, Лев Парцхаладзе й Ірина Геращенко.

***

22.03.2019

Торгували Україною у прямому ефірі: у соцмережах обурені переговорами Бойка з Медведєвим у Москві

Користувачі соціальних мереж, політики та експерти обурені візитом кандидата у президенти України Юрія Бойка та одіозного політика Віктора Медведчука у Москву, де вони провели переговори з прем'єр-міністром Росії Дмитром Медведєвим та головою «Газпрому» Олексієм Міллером (Прямий).

***

25.03.2019

Павло Петренко: Мін'юст запустив просвітницький проект для молоді «Гусь йде на вибори»

25 березня Міністерство юстиції запустило ініціативу «Гусь йде на вибори», покликану долучити українську молодь, які сприймають інформацію здебільшого через соціальні мережі й мережу Інтернет, до виборчого процесу та надати молодим українцям інформацію про те, як реалізувати своє право обирати.

Докладніше

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

13.03.2019

Facebook набирает издателей для новых шоу на Facebook Watch

Платформа Facebook Watch с каждым днем набирает обороты, а материнская компания делает все, чтобы это происходило быстрее и качественнее. Теперь, к примеру, у Марка Цукерберга работают над программой, через которую к созданию новых шоу будут подключать крупных издателей, среди которых – компании BuzzFeed и Condé Nast (InternetUA).

У программы пока нет названия, но в Facebook ее называют Facebook match – видеоинкубатор для финансирования сотрудничества создателей видеоконтента и издателей. На данный момент в ней участвуют 12 издателей, причем у двоих из них – BuzzFeed и Condé Nast – уже есть примеры успешной работы. Первый создал коллаборацию со звездой YouTube Ханной Харт, а второй – с певицей Кеке Палмер и актрисой Анджелой Кинсли.

Но если раньше это были, скорее, единичные случаи, то в 2019-м Facebook планирует усилить это направление. Согласно предыдущему отчету DigiDay по этой программе, соцсеть готова тратить до $200 тыс. за шоу. Самое интересное, что при этом права на контент остаются у его создателей, а Facebook лишь получает возможность его показа в течение определенного времени. По его истечению авторы смогут распространять свой контент и на других площадках.

Что ж, неплохая задумка. Возможно, когда-нибудь Марк Цукерберг распространит ее и на украинский рынок, и тогда постарайтесь не упустить свой шанс.

***

15.03.2019

Максим Саваневський

Україна стала однією з 5 країн, де Facebook почав моніторити політичну рекламу

Починаючи з 18 березня Facebook запускає процедуру підтвердження політичної реклами в Україні. Тобто менше, ніж за 2 тижні до завершення першого туру виборів. Окрім України, схожий моніторинг відбувається лише у США, Великобританії, Індії та Бразилії.

Докладніше

***

18.03.2019

Facebook раскрыла технологии аппаратного ускорения своей инфраструктуры

На мероприятии Open Compute Summit в Сан-Хосе (штат Калифорния), Facebook рассекретила три ключевых элемента своей аппаратной инфраструктуры, включая мощный сервер Zion, предназначенный исключительно для тренировки моделей глубокого обучения, и два разработанных компанией самостоятельно чипа – ускорителя специализированных рабочих нагрузок.

Докладніше

***

18.03.2019

ПриватБанк запустил KyivPasTransBot для оплаты проезда в транспорте

ПриватБанк запустил бота KyivPasTransBot для быстрой оплаты проезда в метро и столичном транспорте с помощью популярного мессенджера Telegram (Espreso.tv).

Приобрести единый электронный билет для проезда в киевском метро и наземном городском транспорте можно в два клика, оплатив с помощью банковской карты или Apple Pay (для пользователей iPhone).

После оплаты в боте появится электронный билет с QR-кодом.

***

19.03.2019

Рекламодатели Facebook просят возврата денежных средств после сбоя в работе соцсети

Некоторые маркетологи говорят, что потеряли десятки тысяч долларов своих клиентов, когда социальная сеть рухнула на прошлой неделе. Перерыв в работе Facebook заставил поволноваться рекламодателей. Дэвид Херрманн, совладелец диджитал-маркетингового агентства Social Outlier, которое, по его словам, ежедневно тратит около 400 000$ на рекламу для клиентов в Facebook, потерял связь с Facebook Ads Manager и всей соцсетью минимум на 12 часов. «Я был просто заблокирован, видя, как снимаются деньги с кредитки», – говорит Херрманн. По его словам, один клиентский счет потратил на рекламу привычные 19 000$, но в результате сгенерировал объем продаж в размере 2 000$, когда он обычно получает продаж на 40 000$-60 000$ ежедневно благодаря своим кампаний в Facebook. «Закрытие создало хаос на аукционе», – говорит Херрманн, добавляя, что некоторые рекламодатели платили 270$ за рекламу, которая обычно стоит 30$. Стоит отметить, что Facebook отложил атрибуцию – это значит, что рекламодатели увидят результаты кампаний спустя дни, а то и недели после их запуска. Представитель Facebook заявил в

электронном письме, что компания не будет комментировать предоставление возмещения денег. Маркетологи говорят, что возвраты редки, и даже когда предоставляются, они, как правило, небольшие. Джейсон Портной, владелец диджитал-маркетингового Jport Media, говорит, что он боится подсчитать возможные потери, которые его рекламные клиенты понесли на прошлой неделе. «Вы наблюдаете за тем, что, как вы знаете, не должно быть запущено, и нет возможности остановить это», – говорит Портной. Несмотря на свои недостатки, Facebook все еще остается самым важным каналом продаж для маркетологов (Marketing Media Review).

***

20.03.2019

Facebook блокуватиме рекламу, яка містить дискримінацію

Facebook блокуватиме рекламу контенту, в якому міститься інформація з дискримінацією людей за різними ознаками (Espreso.tv).

Користувачі розкритикували соцмережу за таргетинг реклами, яка містить дискримінацію щодо раси, віку та статі. Компанія отримала ці скарги і почала займатись способами блокування дискримінаційної реклами житла, роботи і кредитів.

Відповідні заходи блокування не дозволять рекламодавцям націлювати рекламований контент на користувачів за ознакою раси, статі, віку. Крім того, реклама таргетингувалась за визначенням поштового індексу.

Американський союз цивільних свобод (ACLU) та інші правозахисні групи подали позов на Facebook і це дозволило отримати гарантії щодо таких дій зі сторони адміністрації соцмережі.

19 березня вони заявили, що «радикальні зміни» обмежать дискримінаційний таргетинг реклами.

***

19.03.2019

Instagram тестирует покупку и оплату товаров в приложении

В рамках тестирования новой функции Instagram разрешил оформлять и оплачивать покупки внутри приложения (InternetUA).

Об этом 19 марта сообщили в информационном центре компании.

«Сегодня мы представляем оформление заказов в Instagram. Когда найдете продукт, который вам нравится, можете купить его, не выходя из приложения», – говорится в сообщении.

Нажимая на понравившийся товар на фото на странице бренда, пользователь должен увидеть кнопку «Оформить заказ в Instagram». Он сможет выбрать размер или цвет и оплатить заказ, не выходя из Instagram.

«Вам нужно всего лишь ввести свое имя, адрес электронной почты, платежную информацию и адрес доставки», – отметили в компании.

В Instagram уверяют, что после первого заказа информация пользователя будет «надежно сохранена» для последующих заказов.

«Вы также будете получать уведомления об отправке и доставке прямо в Instagram, чтобы отслеживать свою покупку», – добавили в компании.

В настоящее время функция тестируется для компаний и доступна пользователям в США. Среди брендов, которые уже используют нововведение, – Adidas, Dior, H&M, MAC Cosmetics, Nike, NYX, Prada, Zara и другие.

***

20.03.2019

Проверка данных заказчиков: Facebook остановил всю политическую рекламу в Украине

Социальная сеть Facebook 20 марта остановила всю политическую рекламу в Украине до подтверждения подлинности данных ее заказчиков. Об этом сообщают Украинские новости (InternetUA).

Отмечается, что теперь Facebook просит заказчика такой рекламы отправить документы для удостоверения личности, несмотря на то, что политические объявления оплачиваются с банковских карт, где уже указан владелец.

Кроме того, документы на украинском языке, в том числе паспорт, не принимаются. Соцсеть требует заграничный паспорт или водительские права международного образца. Процедура подтверждения компанией займет от 48 до 72 часов.

Facebook таким образом пытается помешать возможному вмешательству в выборы-2019 через соцсети.

Также политические рекламные объявления, касающиеся выборов, в соцсети смогут разместить только рекламодатели, которые непосредственно находятся в этой стране.

***

21.03.2019

WhatsApp готовит бизнес-версию своего приложения для iOS

По данным WABetaInfo, приложение WhatsApp Business появилось в App Store в некоторых странах. WhatsApp запустил свое бизнес-приложение на Android еще в начале прошлого года, но он так и не сообщил, когда оно появится на iOS (InternetUA).

Представители популярного мессенджера продолжают молчать и сейчас, однако владельцы iPhone из Мексики уже заметили приложение в App Store. В Аргентине, Бразилии, Германии, Франции, Парагвае, США WhatsApp Business пока не доступен.

В комментариях к записи WABetaInfo в Twitter пользователи, обнаружившие приложение, советуют не искать его через стандартный поиск.

Для этого они предлагают сначала найти сам мессенджер и пролистать его страницу вниз. Бизнес-версия WhatsApp располагается в Похожих приложениях.

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

13.03.2019
Групповые звонки в Viber доступны на всех платформах

Групповые аудиозвонки, анонсированные ранее во время масштабного обновления Viber версии 10, теперь доступны на платформах iOS и Android для пользователей по всему миру (Украинский телекоммуникационный портал).

Долгожданная функция позволяет всем, кто уже обновил приложение, совершать звонки в группе до 5 человек одновременно.

Теперь можно как добавить людей в процессе звонка, так и организовать новый звонок с участниками группового чата.

Функция позволяет сэкономить время, когда нужно быстро поделиться эмоциями с друзьями или же обсудить срочные планы.

Кроме того, групповые звонки с легкостью помогут в деловой коммуникации, позволив созвониться с коллегами/партнёрами из разных точек мира/страны.

***

18.03.2019
В мессенджере WhatsApp появятся две важные функции

Как и большинство компаний, WhatsApp тоже тестирует свои новые функции на ограниченном круге пользователей в специальных бета-версиях приложения. Одними из последний функций, тестированием которых занимается дочерняя компания Facebook, есть встроенный прямо в приложение браузер и обратный поиск изображений.

Докладніше

***

17.03.2019
Пять вещей, которым Facebook должен научиться у WeChat

Недавно Марк Цукерберг рассказал о том, каким видит ближайшее будущее Facebook. Он обещает сфокусироваться на личном общении и приватности. По мнению некоторых экспертов, грядущие изменения сделают социальную сеть похожей на крупнейший китайский сервис WeChat, который

принято называть мессенджером. Но на самом деле это нечто значительно большее.

Докладніше

***

19.03.2019

В Skype появился предпросмотр файлов

Участникам программы Skype Insider предложено протестировать новую функцию предпросмотра отправляемых изображений, видеозаписей и прочих файлов. Кроме того, к файлам теперь можно прикреплять описание, к групповым звонкам подключать до 50 человек, а видео на YouTube смотреть, не отвлекаясь от чата (Украинский телекоммуникационный портал).

Новая функция позволит просмотреть загруженные в программу файлы ещё до отправки и лишний раз убедиться, что они выбраны верно. Файлы разместятся в области ввода сообщения, но сразу отправлены не будут. При желании к ним можно прикрепить текстовое сообщение или краткое описание.

Сейчас предварительный просмотр тестируется только в Skype для персональных компьютеров (8.42.76.37), но позднее обещается и для мобильных устройств.

Немногим ранее на всех платформах инсайдерам стала доступна возможность приглашения к групповым звонкам до 50 участников, что в два раза больше ранее действовавшего лимита. Чтобы не беспокоить полсотни человек в каком-нибудь офисе одновременным воспроизведением рингтона, приглашение к групповому звонку теперь возможно при помощи уведомлений.

В Skype Preview для Android и iOS реализована возможность просмотра видео на YouTube в небольшом плавающем окне, не отвлекаясь от чата с друзьями. Рядовым пользователям Skype все эти новшества станут доступны в ближайшие недели, какие-то конкретные сроки не называются, как обычно.

***

20.03.2019

Facebook готовит отдельное приложение для игр

В компании анонсировали новую вкладку Facebook Gaming для основного мобильного клиента, а также отдельное специализированное приложение для пользователей смартфонов. Утверждается, что там пользователи смогут находить интересующие их игры, стримы, тематические группы и так далее.

Докладніше

***

22.03.2019

В чатах Facebook Messenger теперь можно отвечать на конкретные сообщения

В Messenger станет проще отслеживать, на какие именно сообщения в групповых чатах отвечают пользователи, пишет The Verge (InternetUA).

Новая функция позволяет отвечать на конкретное сообщение, включая медиафайлы и эмодзи. Например, пользователю больше не придётся искать по всему диалогу, кто ответил на заданный им вопрос.

Чтобы ответить на определённое сообщение, нужно удерживать палец на нём. К ответу будет прикрепляться цитата оригинала. Функция развёртывается для пользователей всех стран.

Данная возможность уже реализована в WhatsApp, который также принадлежит Facebook.

***

25.03.2019

Telegram позволил удалять чужие сообщения и переписки без ограничения по времени

В мессенджере Telegram появилась возможность удалять сообщения, даже отправленные собеседником, без ограничений по времени (InternetUA).

Подобная функция появилась ещё в 2017 году, однако тогда она давала возможность удалять только собственные сообщения и только в течение 48 часов.

Теперь пользователи смогут удалять любые свои сообщения в любой момент, в том числе для собеседника, а личные переписки теперь можно удалить целиком у обоих собеседников (речь только про личные переписки).

Другая функция приватности, появившаяся в обновлении – скрытие отправителя при пересылке сообщений. Раньше все пересылаемые сообщения имели кликабельную подпись, однако теперь пользователь может отключить переход по имени на свой профиль.

В Telegram заявили, что таким образом можно «лишить собеседников возможности доказать, что вы им что-то писали». Кроме того, пользователь может выключить отображение своих аватарок, которые отображаются при переходе в профиль по ссылке из подписи у пересылаемых сообщений.

ДОДАТКИ

Додаток 1

18.03.2019

В мессенджере WhatsApp появятся две важные функции

Как и большинство компаний, WhatsApp тоже тестирует свои новые функции на ограниченном круге пользователей в специальных бета-версиях приложения. Прежде чем добавить эти функции в финальную сборку и предоставить всем пользователям доступ к новым функциям, компания должна убедиться, что все работает и выполняет свою задачу должными образом. Одними из последний функций, тестированием которых занимается дочерняя компания Facebook, есть встроенный прямо в приложение браузер и обратный поиск изображений (InternetUA).

Как понятно из названия, первая функция позволит пользователям загружать веб-страницы по ссылке из сообщения прямо внутри приложения, чтобы не переходить постоянно от мессенджера к браузеру и обратно. Наконец, в WhatsApp появится встроенный браузер, ведь у всех остальных мессенджеров он уже давно есть и его значимость и функциональность переоценить сложно.

Единственным пока выявленным ограничением новой функции станет невозможность записи экрана и скриншотов внутри приложения (как в самом мессенджере, так и в браузере), так как WhatsApp себя позиционирует в качестве хорошо защищенного мессенджера. К положительным сторонам новой функции можно отнести специальное предупреждение, когда вы попытаетесь перейти на небезопасный ресурс и то, что ни Facebook, ни WhatsApp не имеют возможности видеть вашу историю просмотров.

Еще одна функция, которую тестирует WhatsApp, получила название Обратный поиск изображений и не самую очевидную функциональность. Если вы получите в чате какое-либо сообщение, вы тут же сможете отправить его в Google на проверку подлинности. То есть в приложении будет кнопка, которая будет отправлять выбранную вами картинку в «Поиск Google по картинке» и убедившись, что она оригинал, не имеющий копий (или, наоборот, подделка), вы сделаете для себя какие-то выводы. Вообще, эта функция должна быть полезна в таких странах, как Индия, и для этой страны ее, наверное, и создали, так как там WhatsApp используется, как главная платформа для распространения ложной информации.

Обе эти функции были обнаружены в бета-версии приложения WhatsApp для ОС Android и в настоящее время недоступны для всех пользователей. Также там нет ни слова о том, если и когда они станут доступны в публичной версии приложения.

(вгору)

Додаток 2

17.03.2019

Пять вещей, которым Facebook должен научиться у WeChat

Для успешного развития соцсеть Марка Цукерберга должна перенимать опыт у китайских коллег. Мобильные платежи, удобная лента новостей и

множество полезных приложений – вот лишь некоторые преимущества «вселенной» WeChat (InternetUA).

На прошлой неделе Марк Цукерберг рассказал о том, каким видит ближайшее будущее Facebook. Он обещает сфокусироваться на личном общении и приватности. По мнению некоторых экспертов, грядущие изменения сделают социальную сеть похожей на крупнейший китайский сервис WeChat, который принято называть мессенджером. Но на самом деле это нечто значительно большее.

Tech in Asia перечисляет главные отличия двух социальных сетей и объясняет, какие опции WeChat пригодились бы Facebook. И одну вещь, которую перенимать точно не стоит.

Упор на личное общение

По словам Цукерберга, Facebook должен стать больше похожим на гостиную, чем на городскую площадь. WeChat уже сейчас соответствует этому описанию. Система основана на обмене личными сообщениями, а не на реальных именах. Аккаунты физических лиц в WeChat непубличны, так что найти в системе человека можно лишь в том случае, если вы знаете его WeChat ID или номер телефона.

Как и в Facebook, пользователи WeChat могут указывать на то, являются ли их сообщения конфиденциальными.

Однако даже если пост общедоступный, посторонние посетители могут увидеть лишь его содержимое, но не комментарии и лайки – они доступны только друзьям.

Подписка вместо ленты новостей

В WeChat есть аналог новостной ленты, в которой пользователь может видеть обновления друзей. В ней также размещаются рекламные сообщения, но не более двух в сутки. Подписки размещаются отдельно и содержат посты из общедоступных аккаунтов.

Недавно в WeChat появилась лента «Главные новости», но при желании ее можно просто не открывать.

Мобильные платежи

Сотни миллионов китайцев используют WeChat для оплаты счетов, заказа еды и пересылки денег. Это одна из главных причин популярности приложения. Чтобы заплатить, достаточно отсканировать QR-код.

Facebook только готовится внедрять электронные платежи. Однако в США системе предстоит выдержать серьезную конкуренцию с Apple Pay, Samsung Pay и Google Pay.

Мини-приложения

WeChat иногда сравнивают со швейцарским ножом: внутри большого приложения есть множество мелких на все случае жизни. В Facebook тоже есть встроенные программы, однако в основном это игры.

Компании придется приложить большие усилия, чтобы изменить эту часть экосистемы и обучить пользователей искать в соцсети приложения, например, для покупок в онлайн-магазине.

Философия сдержанности

WeChat сильно отличается от других интернет-сервисов Китая. Запустив приложение, пользователь не увидит полноэкранную рекламу или всплывающие сообщения, требующие оплатить подписку для получения дополнительных опций. Это проявление философии сдержанности, которой придерживается создатель сервиса Аллен Чжан.

По его словам, WeChat должен приносить пользу, а не удерживать людей любой ценой.

Тем не менее, у WeChat есть целый ряд проблем. Некоторые жители Китая жалуются, что сервис стал слишком вездесущим, а другие указывают, что переписку могут читать спецслужбы. Действительно, сервис не использует сквозное шифрование для защиты сообщений. И если Facebook движется в сторону WeChat, как раз эту часть копировать не стоит.

Если президентские выборы в США в 2020 году выиграет сенатор Элизабет Уоррен, Facebook и другие технологические гиганты ожидают серьезные проблемы. Политик уверена, что IT-гиганты превратились в монополии нового типа, которые следует разделить.

(вгору)

Додаток 3

20.03.2019

Facebook готовит отдельное приложение для игр

Крупные технологические компании на сегодняшний день проявляют повышенный интерес к играм. Доказательством этого являются многочисленные анонсированные или уже запущенные потоковые сервисы, модная тема трассировки лучей и растущая популярность стриминговых платформ. Facebook не является исключением из этого правила. По данным ресурса, каждый месяц более 700 миллионов человек в социальной сети смотрят игровые видео, играют в игры или иначе взаимодействуют с игровым контентом (InternetUA).

Потому в компании анонсировали новую вкладку Facebook Gaming для основного мобильного клиента, а также отдельное специализированное приложение для пользователей смартфонов. Утверждается, что там пользователи смогут находить интересующие их игры, стримы, тематические группы и так далее.

На первых порах новая функция Facebook Gaming будет запущена для тех пользователей, которые проявляли интерес к игровому контенту, а затем расширится на весь мир. При этом пользователи, которые не могут найти вкладку на своей главной панели навигации, обнаружат её в меню «Закладки».

Кроме того, на Android уже идёт бета-тестирование автономного приложения Facebook Gaming, которое предложит больше функций, чем вкладка. Само приложение уже можно скачать, хотя в нём возможны ошибки.

На данный момент не уточняется, когда компания запустит релизную версию повсеместно, однако, скорее всего, затягивать с этим не будут. Учитывая недавний глобальный сбой в работе социальной сети, компании очень нужно реабилитироваться в глазах пользователей. Нововведение Facebook Gaming вполне может подойти на эту роль.

(вгору)

Додаток 4

25.03.2019

Павло Петренко: Мін'юст запустив просвітницький проект для молоді «Гусь йде на вибори»

25 березня Міністерство юстиції запустило ініціативу «Гусь йде на вибори», покликану долучити українську молодь до виборчого процесу та надати молодим українцям інформацію про те, як реалізувати своє право обирати. Ініціатива реалізовується у партнерстві з ілюстратором і автором «Гуся» Надією Кушнір та проектом «Доступна та якісна правова допомога в Україні» у рамках загальнонаціонального правопросвітницького проекту Мін'юсту «Я МАЮ ПРАВО!» (Урядовий портал).

«Сьогодні ми презентуємо надзвичайно важливий і цікавий інструмент донесення інформації до молодих українських виборців, які сприймають інформацію здебільшого через соціальні мережі й мережу Інтернет. Ми презентуємо низку інформаційних роликів «Гусь йде на вибори», головним героєм яких є дуже популярний в мережі персонаж «Гусь». Він роз'яснює, як скористатися своїм правом голосу, як піти на виборчу дільницю й перевірити, чи є ти в списках, як проконтролювати законність волевиявлення й куди звернутися у разі порушень», – наголосив Міністр юстиції Павло Петренко.

Він повідомив, що сьогодні презентовано перший ролик, який стосується права виборця перевірити себе у списках виборців. Впродовж тижня буде презентовано 3 інші відеоролики, в яких «Гусь» розповість про те, як прийти на вибори, проголосувати та як діяти у разі, якщо ви помітили порушення.

«Ми розраховуємо, що ця інформаційна кампанія не лише підніме українцям настрій, а й дасть нашим громадянам додаткову інформацію, щоб вони могли скористатися своїм основним конституційним правом – прийти на вибори й проголосувати», –зазначив Міністр юстиції.

Очільник Мін'юсту нагадав, що відомство спільно з Центральною виборчою комісією наприкінці минулого року розпочало великий просвітницький проект «Я маю право голосу».

«Його мета – зробити так, щоб максимальна кількість українських громадян скористалися своїм конституційним правом обирати майбутнє країни», – підкреслив Павло Петренко.

Менеджер українсько-канадського проекту «Доступна та якісна правова допомога в Україні» Оксана Кікоть наголосила, що правопросвітництво і

посилення правової спроможності є одним з найважливіших напрямків діяльності проекту.

«Ми вже кілька років послідовно й системно співпрацюємо з Міністерством юстиції та системою безоплатної правової допомоги, щоб люди в Україні не лише знали про свої права, а й вміли ними користуватися і знали, як їх захищати, якщо така потреба виникає», – сказала вона.

На її переконання, «Гусь» своєю простотою, креативністю й наочністю подачі інформації допоможе привернути увагу молоді до власних виборчих прав.

За словами авторки «Гуся» Надії Кушнір, багато її однолітків не впевнені, чи варто їм йти на вибори.

«Я рада, що таким чином ми зможемо спонукати молодь до того, щоб скористатись своїм правом й проголосувати на виборах. Адже нам всім тут жити далі, й вже зараз потрібно думати про майбутнє», – наголосила ілюстратор.

(вгору)

Додаток 5

15.03.2019

Максим Саваневський

Україна стала однією з 5 країн, де Facebook почав моніторити політичну рекламу

Починаючи з 18 березня Facebook запускає процедуру підтвердження політичної реклами в Україні. Тобто менше, ніж за 2 тижні до завершення першого туру виборів. Окрім України, схожий моніторинг відбувається лише у США, Великобританії, Індії та Бразилії (Watcher).

Нові правила суттєво ускладнять роботу українських політиків в інтернеті, адже тепер доведеться світити суми грошей, потрачені на рекламу. Імовірно, частина бюджетів перейде з Фейсбука/Інстаграма до Google, який поки що не виставляв таких вимог до ідентифікації рекламодавців.

Отже, що має змінитись в політичній рекламі в Україні з 18 березня.

Вся політична реклама буде маркуватись повідомленням «Paid for by…» – тобто буде вказуватись, хто заплатив за політичну рекламу.

До 18 березня сторінки, які запускають політичну рекламу, зобов'язані пройти процес ідентифікації.

Процес ідентифікації детально описано тут: https://www.facebook.com/business/m/one-sheeters/ads-with-political-content-ukraine.

В разі, якщо ви хочете запускати політичну рекламу, необхідно підтвердити свою особистість.

Процес підтвердження можна зробити ось тут: facebook.com/id або в розділі налаштувань у мобільному додатку Facebook.

Процес перегляду документів триватиме до 48 годин. Тому якщо ви плануєте щось запускати вже 18 березня, треба стартувати вже.

Для підтвердження особистості потрібно:

– обов'язково ввімкнути двофакторну авторизацію;

– обрати одну з опцій ідентифікації: офіційний документ, випущений урядом (паспорт, права) або нотаріальна форма, яку можна завантажити ось тут facebook.com/id.

Процес ідентифікації «Paid for by»

Процедура установки дисклеймерал «Paid for by» відбувається через таб Authorizations в розділі налаштувань сторінки, і шляхом приєднання рекламних акаунтів, які ви плануєте використовувати для реклами сторінки. Процедура налаштування дисклеймерів відбувається на рівні сторінки, а не рекламного кабінету. Цю процедуру можна здійснити лише на десктопній версії соцмережі.

Вимоги до дисклеймера:

– Чітке ім'я

– Не можна використовувати абревіатури

– Не можна використовувати лінки

– Відповідність вимогам:

https://www.facebook.com/policies/ads/restricted_content/disclaimers

Бібліотека реклами

Facebook створив Бібліотеку політичної реклами (https://www.facebook.com/ads/archive/). Вся реклама, яка буде ідентифікуватись, як політична, буде зберігатись в бібліотеці протягом 7 років. Бібліотека реклами буде також агрегувати інформацію про те, як реклама поширювалась – налаштування таргетингу, кошти, витрачені на рекламу і т. д.

(вгору)

Додаток 6

18.03.2019

Facebook раскрыла технологии аппаратного ускорения своей инфраструктуры

На мероприятии Open Compute Summit в Сан-Хосе (штат Калифорния), Facebook рассекретила три ключевых элемента своей аппаратной инфраструктуры, включая мощный сервер Zion, предназначенный исключительно для тренировки моделей глубокого обучения, и два разработанных компанией самостоятельно чипа – ускорителя специализированных рабочих нагрузок (Компьютерное Обозрение).

Zion помогает ускорить наиболее ресурсоёмкую фазу большинства проектов ИИ. В нем используются восемь центральных процессорных модулей. Каждый из них оснащён большим объёмом оперативной памяти DDR и может делиться ею с другими процессорами для координированной обработки данных.

Администраторы могут комплектовать этот сервер восемью дополнительными чипами, оптимизированными для особых типов тренировки ИИ. Эти ускорители основаны на OAM, технологии, которую Facebook открыла для публичного доступа одновременно с ними. OAM это аппаратный стандарт для монтажа разных типов микросхем в общем, стандартизованном модуле.

Применение OAM обеспечивает серверу Zion значительную гибкость и универсальность. В него можно устанавливать графические карты, массивы программируемой логики и процессоры любой конструкции, если все они смонтированы в одинаковых стандартных модулях.

«Zion разделяет компоненты с интенсивным использованием памяти, вычислений и сети, позволяя масштабировать их независимо, – пишут инженеры Facebook Кевин Ли (Kevin Lee), Виджай Рао (Vijay Rao) и Уильям Кристи Арнольд (William Christie Arnold). – По мере роста размера и сложности наших тренировочных нагрузок ИИ, платформа Zion может масштабироваться вместе с ними».

Один из двух чипов, которые компания открыла вместе с Zion, называется Kings Canyon. Он специализирован для ускорения процесса построения умозаключений (inference) моделями ИИ. Facebook использует его в выделенных «ускорительных стойках», которые содержат сразу множество таких чипов и связываются с серверами ЦОД по сети.

Другой чип, Mount Shasta, оптимизирован на аппаратном уровне для транскодирования видео. Он снижает разрешение клипов, загруженных пользователями в социальную сеть, делая видеоконтент более доступным для подписчиков с медленным или ненадёжным подключением к Интернету.

«В среднем мы ожидаем, что эти видеоускорители окажутся во много раз эффективнее наших нынешних серверов», – пишут инженеры Facebook.

(вгору)

Додаток 7

14.03.2019

Ученые рассказали, чем соцсети вредны для здоровья

Интернет и соцсети сопровождают нас весь день, начиная с раннего утра. Шестьдесят один процент владельцев смартфонов начинает пользоваться гаджетом менее чем через пять минут после пробуждения, восемьдесят восемь процентов – менее чем через полчаса, сообщает Хроника.инфо со ссылкой на podrobnosti.ua (InternetUA).

Мы проверяем соцсети, читаем новости, открываем почту сразу после отключения будильника. С одной стороны, это служит сигналом мозгу, что настало утро, пора просыпаться и включаться в работу. С другой – информация начинает поступать слишком резко. Вы наверняка замечали, что после пятнадцатиминутного утреннего серфинга по Сети вы чувствуете себя разбитым, хотя только что проснулись. Этому есть объяснение.

«Быстрое переключение после сна на внимательное изучение ленты новостей и соцсетей вызывает стресс в организме. Кроме этого, большое количество информации, которое обрабатывает мозг до того, как вы полностью проснулись, может снижать способность выстраивать приоритеты в течение дня», – говорит психиатр и доктор медицины Николь Бендерс-Хади.

Если вы постоянно не успеваете выполнять все намеченные дела, вам стоит подальше отложить телефон с утра. Тристан Харрис, бывший специалист по дизайн-этике в Google и соучредитель Center for human technology, полагает, что начиная свой день с телефона, мы вспоминаем о тех задачах, которые не сделали вчера. Это делает человека менее продуктивным. Кроме этого, острое желание проверять соцсети сразу после пробуждения может говорить о зависимости.

Попробуйте проводить первый час после пробуждения без смартфона. Это поможет оставаться более сконцентрированным и спокойным в течение дня. Чтобы отучить себя смотреть в телефон после пробуждения, купите обычный будильник, а смартфон заряжайте далеко от кровати или в другой комнате. Телефон с новостями и рабочими вопросами лучше брать в руки после завтрака – листание ленты во время еды приводит к перееданию. После пробуждения сделайте зарядку, запишите свои мысли или помедитируйте.

(вгору)

Додаток 8

14.03.2019

Как репосты в соцсетях влияют на поведение человека

Ежедневно в Facebook публикуют свыше четырех миллиардов сообщений, в Twitter – порядка пятисот миллионов. Причем больше половины – это репосты. Так люди делятся интересной, с их точки зрения, информацией (InternetUA).

Почему одни сообщения распространяются с невероятной скоростью, а другие остаются практически незамеченными, как репосты влияют на поведение человека – читайте в нашем материале.

Борьба за ценности

Исследователи из Университета Пенсильвании заинтересовались, что побуждает человека делать репост. Для этого они попросили 80 человек в течение нескольких часов читать заметки с сайта газеты The New York Times и решать, будут они ими делиться на своей странице в фейсбуке или нет. Все это время с помощью функциональной магнитно-резонансной томографии нейробиологи следили за активностью мозга испытуемых.

Если участник эксперимента хотел расшарить сообщение (от английского to share – передавать дальше, делиться), в его мозге активизировались сразу несколько областей – медиальная префронтальная кора, кора задней части поясной извилины, предклинье, височно-теменной узел и правая верхняя височная борозда. Эти участки связаны с регуляцией социального поведения и

прогнозированием последствий текущих действий как с точки зрения индивидуальных ценностей, так и общественных установок.

Результаты опыта говорили о том, что картина мозговой активности лучше предсказывает вирусность той или иной статьи, чем осознанное намерение поделиться ею. Исследователи сравнили список заметок, которые участники эксперимента хотели бы опубликовать на своей странице, с реальными репостами в социальных сетях. Самыми популярными в фейсбуке оказались те статьи, чтение которых вызывало наибольшее усиление активности в «ценностных» зонах мозга добровольцев. А вот заявленное на словах желание поделиться заметкой не всегда означало, что статья станет популярной.

Репостнуть и забыть

Согласно работе китайских ученых, излишнее увлечение репостами может негативно сказаться на памяти и способностях к обучению. К такому выводу пришли исследователи, заставив 80 студентов Пекинского университета читать сообщения из социальной сети Weibo – китайского аналога Twitter. Часть испытуемых могли поделиться постами, другие выступали только в роли читателей.

Затем участникам эксперимента дали тест с вопросами о содержании прочитанного. У тех, кто активно репостил заинтересовавшие их сообщения, результаты были примерно в два раза хуже, чем у добровольцев, не имевших такой возможности. Хуже всего студенты запоминали ту информацию, которой они поделились в социальных сетях.

Спустя некоторое время эксперимент повторили, немного усложнив его. После работы с сообщениями из Weibo испытуемым предложили прочитать статью из научно-популярного журнала New Scientist и пройти тест на понимание этой заметки. И опять более высокие результаты были у тех, кто не делился записями в социальных сетях.

Ученые объясняют полученные данные тем, что любители репостов испытывают когнитивную перегрузку: решение о том, делиться информацией или нет, требует некоторых усилий. Это мешает понимать смысл прочитанных сообщений и в целом ухудшает сам процесс обучения.

Выводы китайских ученых косвенно подтверждает работа их коллег из США и Нидерландов. Проанализировав успеваемость 219 студентов американских университетов, они выяснили, что оценки тех, кто во время подготовки к экзаменам пользовался соцсетями, в среднем на 20 процентов ниже, чем у их товарищей, полностью посвятивших себя образовательному процессу.

Искажение реальности

Согласно данным ученых из Колумбийского университета, 72 процента студентов колледжей доверяют ссылкам и сообщениям, полученным от друзей. В том числе они готовы принять на веру и откровенно ложную информацию, если она приходит от кого-то из сетевых контактов.

Большинство пользователей, как правило, расшаривают сообщения от друзей, а от тех, кто придерживается противоположных взглядов, отписываются. Вот почему откровенные фейки, например, о вреде прививок, распространяются среди сетевых единомышленников с молниеносной скоростью. Человек оказывается в своеобразном информационном пузыре, что может серьезно влиять на то, как он воспринимает реальность.

Наиболее уязвимы в этом отношении люди преклонного возраста. Как обнаружили исследователи из Нью-Йоркского и Принстонского университетов, среди пользователей фейсбука старше 65 лет 11 процентов репостят ложную информацию, в то время как среди 18-29-летних таких только три процента.

На позитиве

Позитивные посты вызывают у пользователей больший отклик, чем негативные, выяснили ученые из Калифорнийского университета в Сан-Диего. Они проанализировали больше миллиарда обновлений статусов среди ста миллионов пользователей фейсбука и обнаружили, что каждый новый негативный пост в среднем порождает 1,29 обновления статуса у друзей первоисточника, а позитивное сообщение – 1,75 обновления.

Активность в социальных сетях связана и с продолжительностью жизни. Наблюдения за 12 миллионами американцев показали, что у пользователей фейсбука риск преждевременной смерти ниже на 12 процентов по сравнению с теми, кто в этой соцсети не состоит. В то же время люди с развитыми социальными контактами, независимо от онлайн-активности, живут дольше тех, кто одинок или чье общение ограничено только интернетом.

(вгору)

Додаток 9

18.03.2019

Ирина Фоменко

The Guardian: зависимость от социальных сетей следует рассматривать как болезнь

Депутаты Великобритании заявили, что зависимость от социальных сетей должна рассматриваться как болезнь. Об этом сообщает The Guardian (InternetUA).

Политики призвали к дальнейшему изучению влияния социальных сетей, но есть веские основания полагать, что такие сайты, как Facebook, Instagram и Twitter, которые постоянно конкурируют за то, чтобы пользователи проводили больше времени на их платформах, могут иметь негативное воздействие на детей.

«Крайне важно, чтобы мы защищали молодых людей, чтобы они были в безопасности и были здоровы, когда они в сети», – заявили парламентарии, считающие, что правительству следует срочно профинансировать долгосрочные исследования, чтобы понять, должно ли быть клиническое определение зависимости от социальных сетей.

Доклад был составлен общепартийной парламентской группой по социальным сетям и психическому здоровью и благополучию молодежи, в которую вошли депутаты, заинтересованные в этой теме. Отчет написан при содействии Королевской организации общественного здравоохранения (RSPH), утвердившей свои выводы после серии слушаний по фактическим данным.

Всемирная организация здравоохранения уже предложила включить игровое расстройство в следующую редакцию своего руководства по Международной классификации болезней, определяя его как психическое заболевание, при котором все больший приоритет «отдается играм, а не другим видам деятельности, в той мере, в какой игры имеют приоритет над другими интересами и повседневной деятельностью».

По мнению ВОЗ, для человека, у которого диагностировано игровое расстройство, должно быть значительное ухудшение личной, семейной, социальной, образовательной или трудовой жизни из-за компьютерных игр в течение не менее 12 месяцев. Депутаты предполагают, что подобное определение может применяться к лицам, которые ведут борьбу с чрезмерным использованием социальных сетей, если исследование показало, что это оправдано.

В докладе также содержится призыв к правительству Великобритании издать официальное руководство по здравоохранению о том, как люди в возрасте до 24 лет могут избежать чрезмерного использования социальных сетей. Кроме того, социальные платформы должны обмениваться анонимными данными с исследователями, чтобы помочь понять влияние их продуктов на молодежь.

Группа под председательством Криса Элмора из лейбористской партии и консерватора Уильяма Рэгга признала, что социальные сети принесли много пользы обществу, включая улучшение доступа к информации о здравоохранении. Тем не менее, члены парламента хотят получить 0,5 % от прибыли социальных сетей для финансирования исследований, образовательных инициатив и разработки более четкого руководства для общественности.

Озабоченность влиянием социальных сетей на психическое здоровье детей значительно возросла в последние годы, особенно после кампании, проведенной родителями 14-летней Молли Рассел, которая покончила с собой в 2017 году. Ее отец заявил, что Instagram «помог убить его дочь», и побудил социальную сеть запретить изображения самоповреждений на своем сайте.

«Это расследование четко выдвигает на первый план серьезные и очень реальные проблемы различных экспертов и молодых людей. Всеобъемлющий вывод заключается в том, что компаниям, занимающимся социальными сетями, необходимо обеспечить защиту уязвимых пользователей и регулирование», – заявила исполнительный директор RSPH Ширли Крамер.

По ее словам, следует уделять приоритетное внимание дополнительным изучениям, «чтобы улучшить понимание вреда для здоровья, а также выгод от

социальных сетей для поколения “цифровых аборигенов”, а само исследование должно поддерживаться отраслью».

В отчете также отмечается растущее понимание тактики, используемой технологическими компаниями для поощрения повторного использования их услуг. Депутаты заявили, что правительству следует обратить внимание на то, «какие аспекты социальных сетей по своей природе вредны для психического здоровья и благополучия молодых людей».

«Вскоре правительство опубликует официальный документ, в котором будут изложены обязанности онлайн-платформ, как эти обязанности должны быть выполнены и что произойдет, если их не придерживаться. Интернет-регулятор, установленная законом “обязанность по уходу” и сбор с социальных сетей – все это меры, которые мы рассматриваем как часть нашей работы», – заявили в Министерстве по вопросам цифровых технологий, культуры, средств массовой информации и спорта.

(вгору)

Додаток 10

20.03.2019

С какого возраста ребенку можно иметь смартфон?

Решение о том, когда дать вашему ребенку его первый смартфон или планшет, гораздо важнее, чем может показаться на первый взгляд. Многие родители на сегодняшний момент просто дают своему ребенку устройство для того, чтобы он смотрел на нем мультики и подобный детский контент (к качеству которого, собственно, тоже возникают вопросы, но это совсем другая история). С одной стороны, использование современных технологий – это всегда хорошо. С другой же слишком раннее формирование зависимости от гаджетов может отразиться на будущем ребенка (Украинский телекоммуникационный портал).

Однако зависимость от использования гаджетов – далеко не единственная проблема, которой стоит уделить внимание.

Социализация

Ряд исследований показывают, что около 50 % детей имеют учетные записи в социальных сетях к 12 годам. При этом нет четкой корреляции между тем, насколько человек общителен в сети и в реальном мире. Исследования не подтверждают снижения активности общения у детей. Но это относится лишь к тем детям, которые начали пользоваться смартфонами в школьном возрасте. Более раннее применение гаджетов все-таки не рекомендуется. Как правило, на сегодняшний день наличие смартфона с приложениями вроде Instagram или Facebook – это дополнительный уровень коммуникации, без которого общение со сверстниками уже может быть не полным.

Кибербуллинг

Довольно молодой термин, означающий, грубо говоря, издевательства в социальных сетях. Согласно данным опросов, около 28 % учеников сообщают,

что в какой-то момент подвергались кибербуллингу. Однако если вам кажется, что лишив ребенка смартфона и соцсетей вы избавите его от этой напасти, это не совсем так. Дело в том, что «обычным» издевательствам также подвергается порядка 25-30% учеников школ. Так что гораздо лучше наладить контакт с ребенком и выстроить доверительные отношения, которые позволят ему рассказать о проблеме без страха, чем что-либо запрещать.

Образование

Сложно переоценить образовательный аспект интернета. Буквально два-три клика отделяет нас от любой информации. В этом плане ребенок, конечно, должен уметь пользоваться поисковыми машинами. Только вот огромные массивы информационных данных таят в себе проблему: существует огромное количество непроверенных источников, которые могут давать ошибочные и даже ложные знания. В данном случае желательно использовать только проверенные лично вами веб-сайты и различные официальные порталы и интернет-библиотеки. Но обучать этому ребенка, опять же, нужно в более или менее сознательном возрасте.

Так что же делать?

На самом деле, во всем нужна последовательность и не нужно бросаться из крайности в крайность. Например, существует масса гаджетов для детей, которые позволят им обучаться использованию современных технологий без дополнительных рисков. Это как особые детские планшеты или телефоны, так и, например, смарт-часы для детей 4-8 лет, которые позволят общаться с несколькими доверенными лицами (а именно с родителями и близкими членами семьи), сокращая при этом дополнительные отвлекающие и опасные факторы.

Далее при поступлении ребенка в школу можно приобрести ему недорогой смартфон для общения с членами семьи и сверстниками. Так что период похода ребенка в первый-второй класс может считаться приемлемым.

(вгору)

Додаток 11

13.03.2019

Ольга Карпенко

В Facebook от имени банков предлагают 50 000 грн за ответы о любимых брендах. Это – мошенничество

На днях пользователи украинского Facebook могли столкнуться с разновидностью мошенничества, которое отличается не так оригинальностью идеи, как качеством исполнения. Мошенники, прикрываясь логотипами известных банков (таких, как «ПриватБанк», «Альфа-Банк», «Ощадбанк» и других), предлагают пользователям ответить на несколько вопросов о себе (вроде бренда смартфона или машины) за существенное вознаграждение. В процессе собирают данные карт, включая номера и CVV (AIN.UA).

Этот вид мошенничества детально описал маркетолог Никита Коваленко из Digital Fox. По его словам, это мошенничество отличается «идеальным исполнением»: пользователю сложно заметить, что что-то не в порядке. Оно работает по такой схеме:

– В ленте всплывает рекламное сообщение с обещанием большой суммы денег за ответы на вопросы. Сообщение проиллюстрировано картинкой с логотипом известного банка, это повышает доверие к посту.

– Запускают рекламу со страниц с названием вроде «Подарки» и подобных (постоянно генерируются новые страницы, они полностью заполнены, оформлены, подвязаны под разные аккаунты с разными картами).

– Реклама ведет на Google-форму, где стоит кнопка перехода на лендинг. «Реклама в Facebook на Google-форму считается благонадежной. А в форме стоит всего одна кнопка – с переходом уже на посадочную страничку, разработанную лучше чем 90 % посадочных страниц в нашей стране, где у вас берут телефон, имейл, фамилию…», – пишет Коваленко.

– Пользователь отвечает на несколько вопросов о любимых брендах. Затем попадает на форму с якобы причитающейся ему суммой выплаты.

– В конце пользователя просят совершить подтверждающий платеж на 100 грн, он подтверждает оферту с уже внесенными в нее персональными данными. Мошенники получают не только деньги, но личные данные и данные карты.

Схема – достаточно устойчивая, пишет Коваленко, поскольку если даже банк пожалуется в саппорт Facebook и страницу уберут, подобные страницы генерируются постоянно. Убрать Google-форму нельзя. Посадочные страницы располагаются на разных хостингах – закрыть их быстро тоже не выйдет. Схема проработана достаточно подробно: даже на уровне «правдоподобных» комментариев от пользователей, у которых якобы возникли проблемы и ответов поддержки.

В «ПриватБанк» редакции сообщили, что действительно в сети активировался новый вид мошенничества – «призовые опросы», где под предлогом выплаты денежных призов за ответы на несколько простых вопросов, мошенники получают доступ к личным финансовым данным участников и списывают деньги с карт.

Как сообщила пресс-служба банка, он никогда не организовывал и не проводит в соцсетях или на других интернет ресурсах викторин или опросов с выплатой денежных призов. Если пользователю пришло предложение об участии в таком опросе якобы от банка, переходить по ссылкам мошенников или указывать свои личные данные нельзя.

(вгору)

Додаток 12

17.03.2019
Ирина Фоменко
Почему Facebook не отключил трансляцию резни в Новой Зеландии

Преступник использовал Facebook, чтобы транслировать в прямом эфире убийство десятков людей в Новой Зеландии. Об этом сообщает Recode (InternetUA).

Но независимо от того, как Facebook – и Twitter, и YouTube, и Reddit, и другие платформы, помогшие распространять изображения и видео с массовой стрельбы в Крайстчерче, которую власти сочли террористической атакой – отвечают на критику в отношении их ролей сегодня, нужно помнить ключевую вещь о платформах – они сделали именно то, для чего они предназначены: позволили людям делиться тем, что они хотят, когда они хотят, с таким количеством пользователей, как они хотят.

Конечно, Facebook не хочет, чтобы убийцы транслировали свои преступления по всему миру. Но компания создала инструмент, который позволяет им делать именно это. И он находится на платформе, которая в основном построена, чтобы позволить людям говорить все, что они хотят, не спрашивая разрешения.

Эта структура платформы является ключом к огромному успеху Facebook как компании – пользователи предоставляют контент, а программное обеспечение Facebook мгновенно распространяет его по всему миру:

«Facebook работает как гигантский бизнес с миллиардом пользователей, поскольку он дает возможность им и рекламодателям загружать все, что они хотят. И тот факт, что Facebook не проверяет комментарии людей, рекламу или что-либо еще прежде, чем это буде опубликовано, также дает юридическую защиту, особенно в США: если на Facebook есть что-то неприятное или незаконное, это не потому, что Facebook разместил это – кто-то разместил это на Facebook».

Все гигантские потребительские платформы, появившиеся в Силиконовой долине за последнее десятилетие или около того, работают одинаково: YouTube и Twitter не подписывают ваши комментарии или видео перед их загрузкой, а Airbnb не проверяет вас раньше, чем вы арендуете дом.

Как отметил Цукерберг в 2017 году, он хочет удалять нежелательный контент после его публикации, и компания заявляет, что заблокировала аккаунт стрелка вскоре после прямой трансляции. Также в Facebook заявили, что в будущем социальная сеть потратит миллиарды на программное обеспечение и людей для борьбы со злоупотреблением.

На прошлой неделе Цукерберг объявил о планах сместить акцент Facebook с публичной ленты новостей на более личную, зашифрованную связь. Вполне возможно, что смена Facebook уменьшит вирусность съемок или других ужасных вещей, но это не помешает тому, чтобы подобные материалы появлялись на платформе.

Но, по словам Цукерберга, Facebook будет следить за злоупотреблениями на своей платформе только после появления публикации, так же, как полиция реагирует на преступления, когда узнает о них.

«Теперь я не собираюсь сидеть здесь и говорить вам, что мы собираемся перехватывать весь плохой контент в нашей системе. Мы не проверяем, что говорят люди, прежде чем они скажут это, и, честно говоря, я не думаю, что наше общество должно хотеть, чтобы мы это делали. Свобода означает, что вам не нужно сначала спрашивать разрешения, и по умолчанию вы можете сказать, что хотите. Если вы нарушите наши стандарты сообщества или закон, то столкнетесь с последствиями», – заявил Цукерберг в 2017 году.

Трудно представить, какие последствия Facebook может навязать человеку, который убил десятки людей в пятницу. И трудно представить, что это больше не повторится.

(вгору)

Додаток 13

18.03.2019

Доказом вини прокурора стало листування у месенджері

Посадовця звільнили через вимагання неправомірної вигоди та розголошення відомостей досудового розслідування особі, причетній до злочину (InternetUA).

Зараз важко уявити цивілізоване суспільство без інтернету, соціальних мереж та месенджерів. Ними користуються як підлітки, так і високопосадовці, бо вони роблять спілкування більш зручним. Проте іноді такі переваги сьогодення можуть зіграти з вами злий жарт чи навіть «виступити проти вас у суді». З'являється все більше цікавих випадків судової практики, коли за фотографіями чиновників у соцмережах намагаються вирахувати, чи не нажили вони незаконних статків. Суддям та прокурорам заявляють відводи через те, що вони необачно підтвердили «дружбу» у Facebook зі стороною у судовому процесі. А емодзі (смайли) стають доказами у судах.

19 лютого 2019 року Верховний Суд у складі суддів Касаційного адміністративного суду відмовив у задоволенні позову прокуророві, який не погоджувався з рішенням КДКП про звільнення його з посади.

До Кваліфікаційно-дисциплінарної комісії прокурорів надійшла дисциплінарна скарга від громадянина на прокурора Дергачівської місцевої прокуратури Харківської області, який нібито вимагав безоплатного отримання дров із лісових запасів державного лісозаготівельного підприємства і з метою отримання цієї неправомірної вигоди інформував працівника лісгоспу про хід досудового розслідування, до якого останній мав пряме відношення.

У СВ Дергачівського відділу поліції перебуває кримінальне провадження за ч. 4 ст. 296 КК України (хуліганство, вчинене із застосуванням предмета, спеціально пристосованого для нанесення тілесних ушкоджень). Вказаний прокурор був процесуальним керівником у цьому провадженні і в подальшому мав би виступати державним обвинувачем у суді. Натомість він інформував обвинуваченого про перебіг кримінального провадження, неодноразово попереджав його про проведення з ним слідчих дій. Більше того, він особисто

передавав йому копії процесуальних документів, відеозапис з реєстратора потерпілого та копії протоколів допиту понятих при огляді місця події. При цьому вказані факти мали місце ще до набуття особою статусу підозрюваного.

Скаржник пояснив, що з прокурором він був раніше знайомий, а коли той став процесуальним керівником у його кримінальному провадженні, став звертатися з приводу безоплатного отримання дров в ДП «Харківська лісова науково-дослідна станція». Втім, позивач, який у цьому лісгоспі працював, відмовив прокурору, пояснивши, що дрова можна лише офіційно придбати.

На підтвердження своєї позиції скаржник надав роздруківки листування з прокурором у програмі Viber, з якого видно, що останній вимагав отримання дров із лісових запасів державного лісозаготівельного підприємства. Також посадовець писав, що здійснює процесуальне керівництво у конкретному кримінальному провадженні саме для того, щоб контролювати його хід та мати доступ до матеріалів, а також вказував, що вже передав фігуранту провадження окремі докази (відеозаписи).

Комісія встановила, що телефон абонента, з яким здійснено листування у месенджері, дійсно належить вказаному прокурору. Крім того, скаржник надав флеш-носій із записами телефонних розмов між ним та нібито прокурором, відповідно до яких останній обіцяє передати йому відеозаписи з місця події з реєстратора потерпілого у даному кримінальному провадженні.

Прокурор пояснив, що справді телефонував працівнику лісництва з приводу офіційного придбання дров для свого знайомого, і той надав йому інформацію про ціну та доставку дров. Підтвердив прокурор і спілкування зі скаржником у месенджері, проте заявив, що це листування в його телефоні відсутнє, і він не може стверджувати, що повідомлення, наявні в роздруківці, дійсно мали місце.

Таке пояснення Комісія оцінила критично і сприйняла як намагання прокурора уникнути відповідальності. Інформування фігуранта про хід досудового розслідування і передачу будь-яких доказів та відеозаписів по кримінальному провадженню до оголошення підозри прокурор заперечив.

Кваліфікаційно-дисциплінарна комісія прокурорів вирішила звільнити вказаного прокурора з органів прокуратури, оскільки його позаслужбові стосунки з учасником кримінального провадження суперечать Кодексу професійної етики та поведінки працівників прокуратури.

(вгору)

Додаток 14

20.03.2019

Сенат США требует объяснений от IT-компаний из-за трагедии в Новой Зеландии

Руководителей Facebook, YouTube, Google и Microsoft вызывают в Сенат на экстренный брифинг – дело в том, что Комитет по внутренней безопасности заинтересовался ситуацией с распространением видео, на котором террорист

расстреливает прихожан в мечети новозеландского города Крайстчерч. Онлайн-платформы не смогли вовремя заблокировать жестокий ролик, из-за чего он мгновенно разошелся по интернету (InternetUA).

Власти жаждут ответ

Ситуацией с мгновенным распространением видео расстрела прихожан в мечети города Крайстчерч, в результате которого погибли 50 человек, заинтересовалось правительство США, сообщает The Verge.

Председатель комитета Сената США по внутренней безопасности Бенни Томпсон направил приглашения в адрес главы Facebook Марка Цукерберга, главы YouTube Сьюзан Войжицки, главы Twitter Джека Дорси и главы Microsoft Сатьи Наделлы, в которых призывает компании Кремниевой долины отчитаться по данному вопросу на брифинге 27 марта.

Томпсон хочет узнать, почему онлайн-платформы допустили живую трансляцию расстрела мирных жителей и позволили перезаливать видео, что привело к беспрецедентному распространению ролика в интернете.

«Я был глубоко обеспокоен, когда узнал, что один из стрелков транслировал эту атаку в прямом эфире в Facebook, а впоследствии этот ролик был повторно загружен в Twitter, YouTube и другие платформы. Видео было широко распространено на ваших платформах долгое время после атаки, несмотря на призывы новозеландских властей удалить его», – заявил председатель комитета.

В письмах-приглашениях говорится о том, что IT-компании должны удалять террористический контент в приоритетном порядке. Кроме того, сенаторы хотят услышать, какие меры будут приняты в Facebook, YouTube, Twitter и Microsoft, чтобы такое не повторялось в дальнейшем. «Вы способны на большее», – пишет Бенни Томпсон.

Представитель Facebook подтвердил, что компания «в скором времени» отчитается перед комитетом, но не уточнил точную дату, а также спикера от компании. В пресс-службе YouTube в ответ прислали предыдущее заявление о масштабах распространения видео расстрела на видеохостинге. В Microsoft и Twitter не смогли предоставить оперативный комментарий.

Не бывает силы без ответственности

Ранее YouTube и Facebook попытались оправдаться после критики в свой адрес за неспособность своевременно заблокировать жестокое видео. Администрация этих ресурсов утверждает, что их модераторы сработали отлично, учитывая количество загруженных копий ролика.

«Объем видео, загруженных на YouTube в следующие сутки после атаки, был беспрецедентным как по масштабу, так и по скорости загрузки – иногда она достигла одного ролика в секунду. В ответ мы предприняли ряд шагов, включая автоматическое отклонение любых отснятых материалов, связанных с насилием, временную приостановку возможности сортировки или фильтрации результатов поиска по дате загрузки и обеспечение того, чтобы результаты поиска по этому событию включали в себя новости из авторитетных источников», – заявили в пресс-службе видеохостинга.

Вице-президент Facebook и заместитель главного юрисконсульта компании Крис Сондерби утверждает, что трансляцию жестокого убийства успели посмотреть менее 200 раз, пока оно было в эфире, и около 4 тыс. раз перед тем, как оно было удалено с платформы.

Первая жалоба на ролик поступила спустя 29 минут после начала стрима. По словам Сондерби, копия видео была размещена на форуме 8chan, который стал главным каналом его распространения.

Новый доклад от Facebook вышел на следующий день после новости о том, как социальная сеть удалила 1,5 млн видео с атакой мечети в Новой Зеландии за первые 24 часа после нападения, включая 1,2 млн роликов, которые были запрещены соцсетью к повторной загрузке.

Тем не менее, принятых мер оказалось недостаточно – ролик продолжал распространяться с пугающей скоростью в первые часы после трагедии, которые считаются самыми критическими.

Премьер-министр Новой Зеландии Джасинда Ардерн призвала социальные сети приложить больше усилий для борьбы с терроризмом.

«Мы не можем просто сидеть сложа руки и признавать, что эти платформы просто существуют и что то, что на них размещается, не является ответственностью их руководства. Они являются издателями, а не только почтальонами. Нельзя получать прибыль и не нести за это ответственность», – заявила глава государства.

(вгору)

Додаток 15

21.03.2019

СБУ фіксує активізацію втручання спецслужб РФ у виборчі процеси в Україні

Служба безпеки України у ході виконання покладених на неї завдань із забезпечення інформаційної безпеки держави фіксує активізацію спецслужб РФ із втручання у виборчі процеси в Україні через використання соціальних мереж для маніпулятивного впливу на електоральні настрої українських користувачів мережі Інтернет (InternetUA).

Фахівці Служби також зафіксували, що з кінця 2018 року напрямки інформаційного впливу з боку російських «кураторів» змістилися у площину масового поширення тенденційної інформації щодо неможливості проведення в Україні чесних виборів Президента, а також розпалювання міжконфесійної ворожнечі на тлі отримання українською церквою Томосу. Разом із тим російські спецслужби продовжують використовувати вектор розповсюдження пропагандистських матеріалів антидержавного змісту.

Співробітники СБУ, зокрема, припинили діяльність розгалуженої мережі антиукраїнських інтернет-агітаторів, до складу якої входило четверо мешканців Миколаєва та четверо одеситів. Учасники мережі поширювали в регіональних та загальнодержавному сегментах мережі Інтернет матеріали із ознаками

сепаратистського змісту, спрямовані на штучне загострення суспільно-політичної ситуації в регіоні напередодні та під час президентських виборів у країні.

За кураторства російської сторони зловмисники поширювали у соцмережі «Вконтакте» через спільноти антиукраїнського спрямування, «News-Front Новороссия Юго-Восточный фронт», «Республика новороссия антимайдан» інформаційні матеріали з ознаками закликів до зміни меж державного кордону України. Учасники мережі отримували за «роботу» матеріальну винагороду через сервіси грошових переказів, що внесені до «санкційного» списку та відповідно заборонені в Україні, зокрема «Золотая корона» та Webmoney.

Служба безпеки України вкотре звертається до українських користувачів Інтернету з проханням бути уважними та у разі отримання від невідомих осіб пропозицій щодо поширення в соцмережах інформації антиукраїнського спрямування повідомляти на гарячу лінію СБ України.

(вгору)

Додаток 16

25.03.2019

WhatsApp получил новую функцию для блокировки чужих аккаунтов

Как бы сильно не старались конкуренты в лице Telegram, Viber и Skype, но потеснить позиции WhatsApp на рынке онлайн-общения им не удается. Отчасти это связано с тем, что разработчики самого популярного в мире мессенджера с ежемесячной аудиторией в более чем 1,5 млрд человек постоянно внедряют в него различные новые функции и возможности. Как стало известно, данный мессенджер в последней бета-версии получил важнейшую новую функцию, а обернуться она может тем, что чужую учетную запись заблокируют (Украинский телекоммуникационный портал).

Вот уже как почти целый год многие страны мира страдают от того, что злоумышленники с подставных номеров распространяют заведомо фейковую и опасную для жизни людей информацию, а еще они вербуют в различные террористические организации, деятельность которых запрещена в России. Служба модераторов не справляется с проблемой, поэтому разработчики WhatsApp решили пойти на радикальный шаг, добавив в свой сервис новую возможность. Она позволит всем пользователям блокировать чужие аккаунты, а происходить это будет очень оперативно.

В версии WhatsApp под номером 2.19.80 содержится скрытая возможность для того, чтобы подать жалобу на какого-либо пользователя, от которого поступило сообщение. Более того, жаловаться можно даже на тех, кто публикует что-то в публичных групповых чатах. В таком случае, если жалоб наберется более десяти в течение суток, информация об активности аккаунта автоматически будет передана модератору. Он ее проверит. Если будут

выявлены какие-то нарушения правил использования сервиса, ученую запись заблокируют.

В таком случае возможность пользоваться WhatsApp на конкретном номере телефона пропадет, и это должно остановить спам и распространение опасной для жизни полностью недостоверной информации. Таким образом, по сути, разработчики предлагают при помощи новой функции блокировать чужие аккаунты. При этом отмечается, что автоматических блокировок не будет, то есть отключать учетные записи станут только после ручной проверки модератором. Это должно исключить вероятность каких-либо случайных ограничений доступ к учетным записям. Подобное новшество совершенно точно сделает самый популярный мессенджер в мире еще более востребованным среди пользователей по всему миру, ведь спама станет меньше.

(вгору)

Додаток 17

13.03.2019

В Facebook невозможно отключить поиск профиля по номеру телефона

Пользователи соцсети недовольны тем, что телефонные номера, которые Facebook требует вводить при прохождении двухфакторной аутентификации, привязываются к их профилям: в результате кто угодно может найти пользователей по их номеру, пишет TechCrunch (InternetUA).

Хуже всего то, что полностью выключить это в Facebook нельзя.

В прошлом году Facebook заставили признаться, что после того, как она месяцами навязывала пользователям F2A по номеру телефона, эти номера использовались для таргетинга рекламы. Теперь пользователи обнаружили, что настройка Facebook позволяет кому угодно – даже людям без аккаунтов в соцсети – осуществлять поиск их профилей по ранее указанным ими для авторизации номерам.

Пользователь может от всех скрыть свой номер в настройках аккаунта. Однако его профиль всё равно можно найти другими способами: например, когда кто-то загружает контактные данные людей со своего смартфона на Facebook. Пользователь может ограничить круг людей, которые будут видеть профиль при поиске по номеру телефона – например, все (это установлено по умолчанию), друзья или друзья друзей, но не стать полностью невидимым.

Это, по мнению экспертов в области, достаточно опасно с учётом распространения такой практики, как SIM-свопинг, когда злоумышленники перехватывают мобильные номера жертв и получают доступ к их аккаунтам. То есть, по сути, инструмент безопасности применяется для того, чтобы снизить приватность пользователей.

Представители Facebook заявили, что настройка не нова, касается любых номеров, привязанных к профилям, и ничего особого в ней нет. При желании

пользователь может настроить двухфакторную аутентификацию без мобильного телефона.

На вопрос о том, позволит ли Facebook пользователям отключить настройку, компания сказала, что не комментирует будущие планы. На вопрос, почему в настройке управления поиском по телефону по умолчанию задано «все», Facebook ответила, что это позволяет легче находить людей, которые ещё не в списке друзей.

(вгору)

Додаток 18

13.03.2019

Киберпреступники атакуют интернет-магазины на базе WordPress

Злоумышленники атакуют интернет-магазины на базе WordPress с помощью бэкдора, которым они заражают сайты через уязвимость в плагине Abandoned Cart Lite for WooCommerce. Согласно данным официального репозитория плагинов WordPress, в настоящее время Abandoned Cart Lite for WooCommerce установлен более чем на 20 тыс. сайтов (InternetUA).

Атаки представляют собой тот редкий случай, когда заурядная и в большинстве случаев безобидная XSS-уязвимость может использоваться для осуществления серьезных взломов. Как правило, межсайтовый скриптинг редко используется в серьезных атаках, но в случае с Abandoned Cart Lite for WooCommerce все обстоит именно так.

С помощью плагина Abandoned Cart Lite for WooCommerce администраторы сайтов могут просматривать содержимое заброшенных корзин и узнавать, какие товары пользователи добавили в них перед тем, как покинуть сайт. Плагин позволяет составлять перечни потенциально популярных товаров, которыми магазину лучше запастись на будущее. Доступ к перечням есть только у администраторов и привилегированных пользователей.

Как сообщает специалист компании Defiant Майки Винстра (Mikey Veenstra), с помощью автоматизации злоумышленники создают на сайтах с уязвимым плагином корзины, содержащие товары с видоизмененными названиям. В одно из полей корзины они добавляют код эксплоита, а затем покидают сайт, для того чтобы код сохранился в его базе данных. Когда администратор просматривает перечень оставленных корзин и доходит до корзины с эксплоитом, выполняется вредоносный код.

По словам Винстры, за последние несколько недель было зафиксировано несколько попыток атак с использованием вышеописанного способа. Злоумышленники применяли эксплоит, загружавший файл JavaScript с адреса bit.ly. В свою очередь, этот файл пытался внедрить на сайт два отдельных бэкдора.

Первый бэкдор создает на атакуемом сайте новую учетную запись администратора. Второй же использует весьма редкую технику. Вредонос составляет список всех загруженных на сайт плагинов и ищет первый, который

был отключен администратором. Злоумышленники не включают его, а заменяют содержимое его главного файла вредоносным скриптом, играющим роль бэкдора для обеспечения доступа к сайту в будущем.

(вгору)

Додаток 19

14.03.2019
Владимир Кондрашов
Эксперты: хакеры проводят «разведку боем» от имени НАПК

13 марта была осуществлена массовая рассылка вредоносных документов (MS Word Document), «вооруженных» макросом. Атака была направлена на украинские органы государственной власти и финансовые учреждения (InternetUA).

Об этом говорится в сообщении частной CERT-компании CyS-Centrum, передает InternetUA.

В качестве приманки использовалось письмо от имени Национального агентства по вопросам предотвращения коррупции.

Что произошло

Как сообщается, при организации рассылки злоумышленники отдельно озадачились обеспечением уникальности каждого вредоносного вложения и email-адреса отправителя.

– В качестве приманки использована «тема» «Національного агенства з питань запобігання корупції». Примечательно, что в заголовке письма «Reply to» указан email-адрес «bogdan_shapka@nazkgov[.]club», который уже фигурировал 25 октября 2017 года в подобной массовой рассылке, когда на атакуемые объекты загружалась вредоносная программа Ursnif (сходство наблюдается также в свойствах использованного SSL-сертификата), – говорится в сообщении компании.

В случае активации содержимого (запуска макроса) на атакуемом ПК будет выполнена команда powershell, которая повлечет за собой цепочку связанных событий, в конечном счете ведущую к заражению ПК вредоносной программой.

Для коммуникации с сервером управления используется HTTPS-соединение (с самоподписанным (от 12.03.2019) сертификатом). Основную логику работы первой фазы заражения выполняют powershell и MSIL байт-код (оригинальное имя: «tools.dll»; дата компиляции: 2019-03-12 06:16:05; класс «R3Rq4b8»). Изначально обеспечивается сбор информации об атакуемом объекте (systeminfo, ipconfig, netstat и др., а также снимок экрана). Вторая фаза предполагает загрузку на ПК другого EXE/DLL файла (на момент исследования не установлен).

Разведка боем?

В CyS-Centrum пока удерживаются от комментариев об атрибуции этой атаки к какой-либо угрозе.

– Несмотря на то, что аналогичные рассылки даже в 2019 году имели место в отношении и других стран, эта кампания может быть разведкой, проведенной боем, – отмечают эксперты.

В пользу данного утверждения говорят география распространения вредоносных документов (Украина), направленность атаки на государственные учреждения, то, что примененные скрипты обеспечивают сбор достаточно большого количества информации об объекте атаки и тот факт, что пока не удалось установить вредоносную программу, которая должна быть загружена с сервера (вместо этого на ПК загружался файл с нулевым размером), это может объясняться либо избирательностью в выборе жертв, либо имитацией загрузки, что весьма характерно для этапа предварительной разведки целей.

Также эксперты отмечают, что злоумышленники, возможно, заинтересованы в атаках на организации среднего и большого размера. В пользу этого предположения говорит тот факт, что одна из выполняемых проверок определяет принадлежность атакованного компьютера к домену (как правило, применяется в корпоративных сетях).

Как уберечься

Применительно к конкретному инциденту, эксперты рекомендуют:

– Ограничить возможность запуска документов с макросами.

– Предотвратить возможность запуска powershell.exe из-под WINWORD.EXE (в данном случае powershell даже не был переименован).

– Обращать внимание на необходимость мониторинга (например, с помощью штатных средств журналирования ОС и/или sysmon) фактов запуска легитимных утилит (процессов), используемых на этапе разведки объекта атаки.

– Обеспечить мониторинг сетевых подключений, осуществляемых с помощью самоподписанных сертификатов.

– В случае выявления фактов коммуникации с упомянутым IP-адресом осуществить исследование инцидента.

Отметим, что это уже не первый случай, когда письма с вредоносом рассылаются от имени НАПК. Ранее мы уже писали о таких фактах в марте 2018 года и октябре 2017-го.

(вгору)

Додаток 20

14.03.2019

Найден единственный способ отличить фальшивую регистрацию через аккаунт в Facebook от настоящей

На различных сомнительных сайтах пользователям выводятся всплывающие окна с предложением зарегистрироваться через Facebook. Эти окна неотличимы от настоящих, но на деле только крадут логины и пароли (InternetUA).

Даже продвинутые пользователи могут попасться

Эксперты по безопасности компании Myki выявили изощренную фишинговую кампанию, которая может сбить с толку даже технически продвинутых пользователей.

Принцип ее действия прост: злоумышленники заманивают пользователей на вредоносные страницы – обычно это либо блоги, либо какие-либо сомнительные интернет-магазины, где выводится всплывающее предложение зарегистрироваться на сайте через Facebook с полями для ввода почтового адреса или телефона и пароля от своего аккаунта в соцсети.

Фальшивое окно неотличимо от настоящего, но на самом деле его единственное предназначение – красть логины и паролей у пользователей.

Опасность в данном случае состоит именно в том, что легитимные окна регистрации через Facebook, выводящиеся на множестве популярных сайтов, выглядят совершенно так же. Метод регистрации или входа в сервис через Facebook чрезвычайно распространен и считается весьма безопасным, не говоря уже о том, что он занимает намного меньше времени, чем стандартная регистрация с использованием адреса электронной почты и вводом различных персональных данных.

Фишеры используют фальшивое окно регистрации в Facebook. Как отличить от настоящего

Злоумышленники тщательно подошли к изготовлению фальшивых всплывающих окон: те же шрифты, то же оформление. Присутствует даже строка с адресом, начинающимся с https://www.facebook.com. Но на деле это имитация, созданная с помощью HTML и JavaScript.

Попробуйте это окно подвинуть

Есть только один действенный способ проверить, настоящее ли это окно Facebook или фальшивка: уменьшить размер окна браузера и попытаться передвинуть «всплывающее» окно за его пределы. Если его часть исчезает за границей окна браузера, значит это фальшивка.

«Весьма эффективный способ «коллекционирования» логинов и паролей к Facebook, особенно учитывая, что далеко не все используют двухфакторную авторизацию, – считает Михаил Зайцев, эксперт по информационной безопасности компании SECConsultServices. – То, что эти фальшивые всплывающие окна проявляются пока только на мусорных и откровенно вредоносных сайтах, утешает мало: в определенный момент злоумышленники могут скомпрометировать какой-либо легитимный ресурс с высокой посещаемостью и встроить соответствующий код в него. В этом случае сотни и тысячи людей могут, сами того не зная, могут «подарить» контроль над своими учетными записями в Facebook хакерам. А те, учитывая распространенность регистрации через Facebook на всевозможных коммерческих ресурсах, смогут нанести весьма существенный ущерб».

(вгору)

Додаток 21

15.03.2019

Две трети антивирусов в Google Play Store оказались ненастоящими

Австрийская организация AV-Comparatives, занимающаяся тестированием антивирусных продуктов, опубликовала отчёт об исследовании, показавшем, что две трети антивирусов для платформы Android выполняют свою работу некачественно или не делают вообще ничего (Компьютерное Обозрение).

Готовя этот отчёт, сотрудники AV-Comparatives в январе 2019 г. тщательным образом проверили 250 антивирусных мобильных приложений из официального магазина Google Play Store.

В индивидуальных тестах исследователи загружали образец вируса через браузер и устанавливали его на реальном устройстве (эмуляторы не использовались). Такую процедуру они проделывали 2 тыс. раз. Все две тысячи подгружаемых вирусов, червей и троянов относились к широко распространённым штаммам, обнаруженным в прошлом году, то есть они давно уже должны были быть проиндексированы антивирусными инструментами.

AV-Comparatives сообщает, что многие из антивирусов не выполняют вообще или имитируют сканирование системы, а ищут вредоносный код по именам файлов, занесенным в их «чёрный список».

При этом, некоторые из них отмечают как угрозу любое приложение, которое не внесено в их «белый список». Из-за этого они, в ряде совсем уж анекдотичных случаев, поднимали тревогу из-за своих собственных файлов, так как разработчики забыли упомянуть их в «белом списке».

AV-Comparatives считала антивирус успешно прошедшим испытания и эффективным, если он выявлял по крайней мере 30 % вредоносных программ (с нулевым ложным срабатыванием). По этому критерию было отбраковано 170 из 250 средств обеспечения безопасности для Android.

Отмечается, что большинство из этих программ, вероятно, разрабатывали любители или организации, которые специализировались в других областях деятельности, и по маркетинговым или иным соображениям хотели добавить в свой портфель предложений антивирус для Android.

Многие из этих подделок имеют одинаковый пользовательский интерфейс, выглядят как будто сошли с одного конвейера и больше нацелены на показ рекламы, чем на поиск угроз.

Экспертов AV-Comparative полностью удовлетворили всего 23 из протестированных приложений, обнаружившие 100 % образцов вредоносного кода. Также они отметили, что 16 инструментов в значительной мере утратили свой защитный потенциал из-за некачественного переноса на Android 8.

(вгору)

Додаток 22

18.03.2019

Манипуляции с DNS и целенаправленные атаки будут наиболее опасными для предприятий

Несмотря на то, что к некоторым видам атак хакеры обращаются из года в год (фишинг и инъекции SQL-кода), в прошлом году злоумышленники начали применять новые методы, рассказали на конференции RSA эксперты SANS Institute. Они выделили пять самых опасных методов атак, с которыми предприятия могут столкнуться в этом году (Компьютерное Обозрение).

В SANS Institute причислили манипуляции с DNS к числу главных векторов атак. Применяя их, злоумышленники используют украденные учетные данные для входа в системы реестра доменов и изменения информации. Чтобы снизить риск манипулирования DNS-запросами, в компании рекомендуют организациям использовать многофакторную аутентификацию и развертывать DNSsec, использующее для обеспечения безопасности процесса преобразования доменных имен цифровую подпись.

Прикрытие доменом (domain fronting, технология сокрытия конечного адреса) применяется злоумышленниками для сокрытия локаций передачи команд и следов взлома. Технология сокрытия конечного адреса позволяет подменять функциональность сети доставки контента в облаке, чтобы принудить системы доверять ему. Чтобы ограничить риск взлома домена, рекомендуется компаниям не доверять слепо трафик (как исходящий, так и входящий) своим облачным провайдерам.

В SANS Institute также предупредили о растущем риске целенаправленных атак. Точечный мониторинг соцсетей и прочих источников позволяет хакерам получить доступ к учетным записям пользователей. В компании предлагают пользователям просмотреть свои облачные настройки в различных ресурсах и принять меры по ограничению доступа к личной информации.

Информация, которая проходит через шлюзы DNS, по умолчанию не защищена, и это открывает потенциальному злоумышленнику возможность просмотреть трафик и понять, куда он направляется. Проблема утечки информации DNS может быть решена путем шифрования трафика DNS через HTTPS.

Baseboard Management Controllers (BMC) – это специальные контроллеры удаленного управления компьютером, интегрированные на материнскую плату. Они являются неотъемлемой частью многих современных ИТ-систем, обеспечивая возможность мониторинга и управления встроенным программным и аппаратным обеспечением. Такие системы обладают уязвимостями, которые могут применяться злоумышленниками. Чтобы снизить риски их эксплуатации, пользователям необходимо удалить ненужные утилиты управления и отслеживать доступ к тем консолям управления, без которых невозможно обойтись.

(вгору)

Додаток 23

18.03.2019

Число утечек данных из медицинских учреждений выросло на 16 % за год

Компания InfoWatch представила свои данные по утечкам конфиденциальной информации из учреждений здравоохранения в прошлом году. Аналитический центр компании зарегистрировал 429 утечек из различных учреждений медицинской сферы по всему миру за год. Это почти на 16 % больше, чем в 2017 г. Число скомпрометированных записей персональных данных за год выросло почти вдвое и составило 27 млн (Компьютерное Обозрение).

Более 80 % записей утекло в результате внешнего воздействия. Так, в начале 2018 г. киберпреступники атаковали информационную систему Юго-Восточной медицинской службы Норвегии. Украдены данные около 3 млн человек, то есть примерно половины жителей этой скандинавской страны. В норвежском управлении по информационной безопасности не исключают, что хакеры действовали по заказу иностранного государства.

Каждая третья утечка в прошлом году произошла в результате хакерских атак, но основными виновниками утечек в данной отрасли остаются сотрудники. На их долю приходится 53,7 % зарегистрированных инцидентов.

Соотношение умышленных и случайных утечек в медицине составило 47,5 % и 52,5 %. При этом среди утечек, совершенных по вине сотрудников, доля умышленных инцидентов составляет немногим более 20 %. В основном данные ограниченного доступа компрометируются в результате ошибок, недосмотра или халатности. Например, в США данные более 200 тыс. пациентов были оставлены на незащищенном FTP-сервере. Виновником утечки названа компания MedEvolve – поставщик управленческого ПО для медучреждений.

Доля персональных данных в утечках по сравнению с 2017 г. сократилась с 90,2 % до 84,4 %. При этом в 2018 г. выросла доля утечек платежной информации – с 8,6 % до 13,5 %. Это может быть связано с развитием коммерческой медицины и новых форм оплаты.

Более 45 % утечек в 2018 г. случились через сетевой канал. Далее располагаются электронная почта (21,1%) и бумажные документы (20,2%). В Великобритании аптечная сеть Well Pharmacy в результате ошибочной рассылки по e-mail скомпрометировала личные данные более 24 тыс. сотрудников и местных жителей. Утекла такая информация, как имена, адреса, номера телефонов, адреса электронной почты и данные о заработной плате.

(вгору)

Додаток 24

18.03.2019

DARPA работает над абсолютно защищенной системой голосования

Министерство обороны США потратит $10 млн на разработку инновационной технологии проведения выборов. Следить за ходом голосования смогут избиратели, а взломать систему будет невозможно: проверять надежность ПО и «железа» будут хакеры со всего мира (InternetUA).

Криптовыборы

Агентство перспективных оборонных разработок США (DARPA) заключило контракт с американской компанией Galois, которая ранее уже выполняла заказы государства. Разработчики планируют создать уникальную систему голосования с открытым кодом. Создатели обещают сделать общедоступным не только ПО, но и технические характеристики «железа», в основу которого лягут недавние разработки DARPA.

Galois создаст два вида прототипов. Первым проектом станет устройство для заполнения бюллетеня. Используя тачскрин, избиратель внесет свой голос в бланк. Затем документ распечатают, после чего его можно будет опустить в урну.

Специальный датчик распознает данные на бюллетене. Штрихкод для этого не понадобится, поскольку сенсор сможет самостоятельно считывать текст на бланке.

После этого избиратель получит специальный криптокод, который потом можно будет «пробить» в базе голосов.

Такой подход позволит гражданским активистам подсчитать реальное количество голосов за каждого кандидата и убедиться, что организаторы выборов не мошенничали в процессе. Любая организация сможет создать независимую программу для подсчета голосов. При подключении к базе она определит, как на самом деле голосовали избиратели.

Вторым проектом Galois станет оптическое устройство для распознавания маркировок на бюллетенях, нанесенных вручную.

Избирательный «полигон»

Как сообщает Motherboard, использовать разработку на выборах агентство не планирует. Платформа станет тестовой лабораторией для оценки надежности технологии.

Прототипы представят на хакатоне Def Con Voting Village в 2019 и 2020 годах. Хакеры и эксперты по безопасности смогут дать свою оценку проекту и проверить, насколько ПО подвержено риску взлома. Также DARPA планирует связаться с университетами, чтобы получить заключение специалистов.

Поскольку все сведения выложат в открытый доступ, любая компания сможет воспользоваться ими. Разработчики надеются, что технологией заинтересуются производители устройств для подсчета голосов.

«Мы не будем внедрять систему самостоятельно. Наша цель – разработать методику, которой смогут воспользоваться другие производители», – пояснил представитель DARPA Линтон Сэлмон.

По его словам, основную ставку агентство делает именно на «железо». Если сделать устройства для проведения выборов и считывания голосов

максимально защищенными, хакеры не смогут воспользоваться уязвимостями в ПО, даже если найти лазейку теоретически возможно.

Машины на страже

В будущем машины для проведения голосований будут препятствовать нарушениям. Они не позволят злоумышленнику взломать «железо», например, используя карту памяти, которая заставит автомат записать 20 голосов вместо одного.

Сэлмон подчеркивает, что проект DARPA и Galois – это только начало.

«Проблема настолько серьезная, что одной программы недостаточно, чтобы решить ее даже на 20 %».

Большинство систем голосования пока далеки от совершенства, но многие государства все равно тестируют их, невзирая на риски. Недавно эксперты обнаружили несовершенства на швейцарской платформе для онлайн-голосования, пилотные испытания которой должны были начаться в марте.

Не одно государство экспериментирует и с системами голосования на блокчейне. Подход тестируют в Швейцарии, США, Южной Корее и Японии, пытаясь разобраться, так ли он эффективен и безопасен, как считалось во времена бума криптовалют.

(вгору)

Додаток 25

18.03.2019
Владимир Кондрашов
Укрпочта засветила в сети конфиденциальные данные

Эксперт по кибербезопасности Александр Галущенко обнаружил в свободном доступе в сети несколько терабайт данных «Укрпочты», среди которых – списки клиентов и почтовых отправлений, финансовая информация компании и другие конфиденциальные данные. По подсчетам эксперта, «дыра» в безопасности, в случае её использования злоумышленниками, могла стоить национальному почтовому оператору полмиллиарда гривен (InternetUA).

18 марта Александр Галущенко на своей странице в Facebook опубликовал информацию о том, что нашел брешь в сети Укрпочты, открывающую доступ к конфиденциальным данным компании:

– Укрпочта. Система платежей. Списки клиентов и почтовых отправлений. Что-то из старого по пенсиям. Некислый объем на несколько тер. Все четко разложено и готово к применению в незаконных схемах. И они рассказывают, что у них деньги не воруют.

Информацию об уязвимости эксперт подкрепил скриншотами с обнаруженного в сети диска с данными Укрпочты и добавил:

– Там есть все, чтобы стать главным системным администратором организации, главным бухгалтером, частично юристом и еще кем-то, в чем я точно не разбираюсь.

В комментарии нашему изданию Александр Галущенко уточнил, что обнаружил информацию на устройстве в одной из областей Украины, где были доступы к системе перевода денег, данным по пенсиям, доступ к бухгалтерии и другим критически важным ресурсам.

Укрпочта довольно оперативно отреагировала на инцидент. Спустя несколько часов после обнародования информации об уязвимости руководитель Укрпочты Игорь Смелянский сообщил, что они проверяют информацию.

– Я попросил наших специалистов разобраться. Они уже и будут контактировать. Это часть работы. Такие инциденты (если это правда) бывают в любой компании, даже той, которая тратит миллиарды на ИТ-безопасность, – прокомментировал Игорь Смелянский.

Эксперт с таким тезисом не согласился, отметив, что обнаруженная брешь – «клинический случай», а её наличие «показывает отсутствие этой самой безопасности как класса вообще».

Также Смелянский получил от Александра Галущенко ссылку на зияющую в сети базу с конфиденциальной информацией. Спустя час уязвимость была закрыта.

– Достойная и адекватная реакция руководителя Укрпочты и всех связанных должностных лиц. Доступ закрыт, – прокомментировал Галущенко.

В свою очередь Игорь Смелянский пообещал наказать виновных:

– Надеюсь, мы ещё кое-кого за такой саботаж посадим. Но тут дело небыстрое.

(вгору)

Додаток 26

19.03.2019
Ирина Фоменко
ЕС принял новый протокол реагирования на крупные кибератаки

Европол 18 марта объявил о принятии нового протокола о том, как правоохранительные органы в Европейском Союзе и за его пределами будут реагировать на крупные трансграничные кибератаки. Об этом сообщает Security Week (InternetUA).

Новый протокол ЕС по реагированию правоохранительных органов на чрезвычайные ситуации должен оказаться полезным (EU Law Enforcement Emergency Response Protocol) в случае крупных атак, таких как WannaCry и NotPetya, которые в 2017 году поразили сотни тысяч систем по всему миру и принесли значительные потери многим организациям.

Протокол, принятый Советом ЕС, является частью проекта ЕС по скоординированному реагированию на крупномасштабные трансграничные инциденты и кризисы в области кибербезопасности, и он будет реализован Европейским центром киберпреступности (EC3) Европола. Основное внимание

уделяется быстрой оценке, обмену информацией и координации международных аспектов расследования.

Протокол охватывает только злонамеренные и криминальные инциденты в киберпространстве – Европол подчеркнул, что он не охватывает ситуации, вызванные стихийными бедствиями, человеческой ошибкой или сбоем системы. Его цель – дополнить существующие механизмы управления кризисами.

Протокол состоит из семи основных компонентов: раннее обнаружение и идентификация крупной кибератаки, классификация угрозы, создание координационного центра для реагирования на чрезвычайные ситуации, ранние предупреждения, план оперативных действий для правоохранительных органов, расследование инцидента и закрытие протокола аварийного реагирования.

«Протокол ЕС по реагированию правоохранительных органов на чрезвычайные ситуации определяет процедуры, роли и обязанности ключевых игроков как внутри ЕС, так и за его пределами; безопасные каналы связи и круглосуточные контактные пункты для обмена критически важной информацией; а также общий механизм координации и устранения конфликтов», – заявили в Европоле.

(вгору)

Додаток 27

21.03.2019

Google добавит в Chrome защиту от слежки со стороны сайтов

Компания Google продолжает совершенствовать методы безопасности для своего браузера. Ведь на сегодняшний день есть множество способов шпионить за пользователями, используя веб-сайты, которые обращаются к определённым API-интерфейсам. Одним из способов, который появился несколько лет назад, стал анализ данных акселерометра смартфона. Для этого использовался API для работы с JavaScript. Такой метод позволял, в частности, определять, находится ли пользователь в машине или поезде, сколько времени он сидит без движения или наоборот ходит. Кроме того, с помощью распознавания походки можно было однозначно определить самого пользователя (InternetUA).

И потому в Google работает над тем, чтобы противостоять этой технологии. Сообщается, что там разрабатывают метод блокировки доступа веб-сайтов к данным гироскопа, акселерометра и датчика освещённости. Эта функция появилась в последней сборке Chrome Canary.

По умолчанию доступ к датчикам включён, однако теперь Chrome будет предупреждать о том, что тот или иной сайт пытается получить доступ к датчикам и сенсорам. Это позволит пользователю разрешать или запрещать работу с такими данными. При этом отмечается, что на Android можно заблокировать доступ к вашим данным о движении пока что на всех сайтах

сразу. То есть функции «белого» и «чёрного списков» пока нет, хотя в будущем она может появиться.

При этом отметим, что в своё время Университетом Иллинойса было проведено исследование, которое подтвердило, что сайты вполне могут шпионить за пользователями через смартфоны. Отмечается, что считывание данных с акселерометров и гироскопов нужно владельцам веб-страниц или рекламодателям. Это позволять распознать пользователя и предложить ему таргетированную рекламу.

Как ожидается, в релизе новая возможность появится в Chrome 75.

(вгору)

Додаток 28

21.03.2019

Ирина Фоменко

Уязвимость в Google Фото позволяет преступникам узнать местоположение жертвы

Уязвимость в веб-версии Google Фото позволяет киберпреступникам узнать подробности истории фотографий пользователя. Об этом сообщает Dark Reading (InternetUA).

Через браузерные тайминг-атаки хакеры могут анализировать данные изображения, чтобы узнать, когда человек посещал определенное место. Это не обычная угроза, и она наиболее эффективна в целевом сценарии, но вредоносный веб-сайт можно использовать и для доступа к фотографиям.

«Google Фото много знает о людях, которые его используют. Служба автоматически помечает каждое изображение с помощью метаданных (дата, координаты местоположения), а механизм искусственного интеллекта обнаруживает объекты и события, которые могут указывать на свадьбу, водопад, закат или ряд других мест. Теги распознавания лиц также присутствуют на фотографиях», – объяснил исследователь Imperva Рон Масас. – «Эта подробная информация может многое рассказать о том, когда, где и с кем был человек».

Масас обнаружил, что конечная точка поиска службы уязвима для атаки, называемой межсайтовым скриптингом или XSS. В подтверждение своей концепции он использовал тег HTML-ссылки для создания нескольких перекрестных запросов к конечной точке поиска. Используя JavaScript, он измерил время, необходимое для запроса к серверу Google Фото и получения в качестве ответа нулевых результатов.

Вот как работает эта уязвимость: преступник должен сначала отправить цели злонамеренную ссылку, пока этот человек находится в Google Фото, путем встраивания вредоносного JavaScript в веб-рекламу, отправки прямого сообщения по электронной почте или через онлайн-мессенджер. Вредоносный код JavaScript создает запросы к конечной точке поиска в Google Фото и извлекает ответы.

Однако, как только жертва закрывает вредоносную страницу, поиск прекращается. «В тот момент, когда вы закрываете сайт, я больше не могу этого делать. Но могу обмануть вас, чтобы вы зашли на другой ресурс в будущем, и продолжу оттуда. Нужно, чтобы вы каждый раз открывали сайт», – пояснил Масас.

По мнению исследователя, это не очень сложная атака, но она имеет наибольшую ценность, если хакер специально нацелен на одного человека. Например, кто-то мог использовать уязвимость, чтобы определить местонахождение высокопоставленного человека или узнать, с кем он проводил время.

(вгору)

Додаток 29

26.03.2019

5 лучших антивирусов на Android

Вредоносное ПО для Android является серьезной проблемой для пользователей самой популярной в мире мобильной операционной системы. Изо дня в день количество угроз для «зеленого робота» только увеличивается, а с учетом того, что по всему миру под управлением Android работает несколько миллиардов устройств, даже целенаправленная атака лишь на небольшой их процент может повлечь за собой серьезные последствия. К счастью, с ростом количества и качества вредоносного ПО, растет функциональность и эффективность антивирусного программного обеспечения. Представляем вам пять лучших антивирусных приложений для Android-устройств (InternetUA).

Mobile Security & Antivirus от ESET

ESET Mobile Security установили на свои телефоны и планшеты более 600000 пользователей. После установки приложение будет сканировать ваше устройство на наличие вредоносных программ и обеспечивать его безопасность в режиме реального времени. У ESET Mobile Security также есть антифишинговые функции, которые будут предупреждать вас о любых вредоносных сайтах, которые вы собираетесь посетить.

Приложение также предоставляет подробный отчет о своей работе, который сообщит вам об обнаружении какого-либо подозрительного ПО, а две специальные функции – Remote Lock и Remote Siren – помогут еще больше обезопасить ваш смартфон. Существует две версии приложения: бесплатная базовая и платная премиум-версия с некоторыми дополнительными функциями, возможностью запланировать сканирование и автоматическим обновлением вирусной базы.

Антивирус AVG для Android

Антивирус AVG зарекомендовал себя как эффективное решение для компьютеров, а теперь решил расширить свои границы и заработать на смартфонах и планшетах. У приложения есть бесплатная базовая версия без необходимости регистрации и оплаты. После завершения установки программа

сразу проверит ваше устройство на наличие вредоносного программного обеспечения. AVG также обеспечивает безопасность вашего устройства в режиме реального времени, блокируя вредоносный код еще до его запуска.

AVG является одним из лучших инструментов для использования в качестве антивируса. У этого приложения имеется не только антивирусный сканер, но и функция, котороя поможет найти ваше устройство, если оно было украдено или потеряно. Кроме того, сканирование в AVG распространяется на текстовые сообщения и сайты, которые вы посещаете. Правда, уже эти функции доступны только в расширенной версии AVG.

Comodo Mobile Security

Comodo Mobile Security новее остальных антивирусных решений в этом списке, но по эффективности оно не уступит никому из них. Comodo не только может сканировать и обнаруживать потенциальные угрозы, но также классифицировать их как опасные, подозрительные и безопасные. Это дает пользователям больше маневров для дальнейших действий, так как они понимают, кокой степени угроза будет активирована, если нажать кнопку «Далее». Также здесь есть планировщик сканирования.

Avast Mobile Security

Мобильный антивирус от Avast предоставляет пользователю множество инструментов для обеспечения безопасности его мобильного устройства, включая основную антивирусную функцию под названием Web shield, которая используется для сканирования сайтов, информирования пользователя о вредоносных URL-адресах, а также имеет функцию советника, которая поможет обезопасить ваши данные и избежать их кражи. Avast также умеет чистить историю браузера, блокировать смартфон в случае необходимости и активировать сирену, чтобы отпугнуть грабителя.

Avast Mobile Security в первую очередь предназначен для сканирования на наличие вредоносного ПО программ, которые уже установлены на ваш смартфон или тех, которые вы только собираетесь установить. Avast был также признан одной из лучших антивирусных программ в 2018 году.

Антивирус Dr. Web Light

Компания Dr. Web выпустила мобильную версию своего знаменитого антивируса для ОС Android. Это приложение помогает защитить ваш смартфон от вирусов и вредоносных программ. Dr.Web имеет множество преимуществ, которые включают высокоскоростное сканирование устройства, гибкую настройку, удобный интерфейс, минимальную нагрузку на систему и защиту от нежелательных входящих вызовов и SMS. Одним из плюсов приложения также является то, что оно абсолютно бесплатно.

Довольно сложно выбрать победителя среди приведенных в нашем топе антивирусных приложений. У каждой программы есть свои особенности и уникальные функции. Как вы уже поняли, чтобы обезопасить себя и свой смартфон от нежелательных угроз, достаточно выбрать из нашего списка приложение, которое вам больше всего подходит своей функциональностью – благо, они все бесплатные и действительно могут вам помочь. Защита

информации в наши дни стала действительно критической проблемой, и антивирусные приложения внесли значительный вклад в то, чтобы сделать нашу с вами жизнь проще и безопаснее.

(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.