СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(28.02–13.03)

2018 № 5

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(28.02–13.03)
№ 5

Засновники:
Національна бібліотека України імені В. І. Вернадського
Служба інформаційно-аналітичного забезпечення
органів державної влади (СІАЗ)

Відповідальний редактор
Л. Чуприна, канд. наук із соц. комунікацій

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2018

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

28.02.2018

Viber запускає нову функцію – глобальні спільноти, які можна монетизувати

Месенджер Viber презентував нову функцію «спільноти» – сервіс для обміну повідомленнями в форматі групового чату, при цьому адміністратори отримують нові опції для модерації дискусії.

Докладніше

***

28.02.2018

Дмитрий Демченко

Что такое Vero – социальная сеть, которую называют убийцей Instagram

Последнее время в западных СМИ активно обсуждают социальную сеть Vero, которая неожиданно набрала большую популярность. Создатели называют ее самой «аутентичной», а некоторые западные СМИ уже окрестили сервис «убийцей» Instagram.

Докладніше

***

2.03.2018

Facebook закрыла эксперимент с дополнительной лентой новостей

Социальная сеть Facebook объявила об окончании начатого в октябре прошлого года эксперимента, в рамках которого компания тестировала разделение ленты новостей на две разные ленты в нескольких странах мира. Сообщение об этом было опубликовано в блоге Facebook.

Докладніше

***

2.03.2018

Twitter запустил закладки для сохранения твитов

Команда платформы микроблогов Twitter объявила о запуске функции «Закладки» (Bookmarks) для сохранения твитов, к которым пользователь хочет вернуться позднее (Новости ИТ).

Этот подход намного логичнее, чем использовать для тех же целей «лайки», как это приходилось делать ранее. «Закладки» в профиле пользователя может просматривать только сам пользователь, в отличии от опции «лайков».

Отметим, что функция закладок была анонсирована еще в октябре 2017 года. «Закладки» постепенно станут доступны в приложениях Twitter для iOS и Android, Twitter Lite, а также на мобильной версии mobile.twitter.com.

«Закладки» доступны через пиктограммку «Поделиться» в твите. Для просмотра сохраненных твитов надо пройти в профиль и выбрать пункт «Закладки». Закладку можно удалить также, нажав «Поделиться» в твите в ленте закладок. Через значок «Еще» в верхней части ленты закладок можно удалить сразу все закладки.

***

3.03.2018

Instagram работает над голосовыми и видеозвонками

Instagram, возможно, готовится к запуску звонков и видеосвязи. К такому предположению пришли журналисты TechCrunch, которые обнаружили в Android-версии приложения Instagram файлы и иконки для функций голосового и видеовызова (IGate).

Впервые слухи о работе Instagram над функцией вызовов возникли в январе 2018 года, но тогда речь шла только о внутреннем тестировании. «Теперь, когда значки кнопок есть в общедоступном APK-файле, компании будет сложно отрицать предстоящий запуск», – пишет TechCrunch.

«Боюсь, что мы не можем это прокомментировать», – сказал представитель Instagram. В издании вспомнили случай, когда в компании сначала отказались комментировать найденную журналистами возможность использования анимированных GIF-изображений в «историях», а через неделю объявили о запуске новой функции.

Запуск голосовых и видеозвонков может сделать Instagram лучшей альтернативой Snapchat, одна из самых популярных функций которого – чат с возможностью видеосвязи, указывает TechCrunch. Instagram не в первый раз копирует опции Snapchat: в августе 2016 года разработчики сервиса запустили похожие самоуничтожающиеся «историй», а в мае 2017 года добавили маски для лиц.

***

5.03.2018

YouTube запустив автоматичні субтитри та геотегування для прямих трансляцій

Функція працює завдяки технології автоматичного розпізнавання мови (LASR). Можливість запускати автоматичні субтитри можна буде вже протягом найближчих тижнів (Watcher).

Також YouTube запустив функцію повторного перегляду чату, щоб можна було слідкувати за бесідою навіть після завершення потокового

трансляції. Повторення онлайн-чату відображатиметься разом із відео, як й під час прямого ефіру.

Окрім цього, YouTube додав можливість створювати теги місцеположень до своїх мобільних прямих трансляцій та завантажених відео. Користувачі можуть тепер переглядати відео з одним і тим самим геотегом, просто натиснувши на нього. Також можна використовувати фільтр геолокації на сторінці результатів пошуку, щоб знайти інші відео з певного місця.

Минулого року YouTube представив функцію Супер Чатів для прямих трансляцій. Відтепер креатори можуть налаштувати цю опцію для своїх каналів, використовуючи сервіс IFTTT (If This, Then That). До Супер Чату можна підключити понад 600 послуг та пристроїв з доступом до інтернету (наприклад, світильники, годівниці для домашніх тварин та гармати для конфетті). Супер Чат уже доступний на настільних комп'ютерах, пристроях Android та iOS.

***

5.03.2018

BuzzSumo: количество шеров в сетях сократилось на 50 % с 2015 года

«Если вы использует подход к контенту трехлетней давности, то он теперь на 50 % менее эффективный», – такие выводы нового исследования BuzzSumo, который проанализировал 100 млн статей, изданных в 2017 году, и обнаружил, что число репостов в соцсетях сократилось на 50 % с 2015 года (Marketing Media Review).

Независимые исследования также обнаружили сокращение реферального трафика с Facebook вслед за изменениями в алгоритме ленты.

Среди ключевых трендов контента:

- Число репостов сократилось наполовину с 2015 года
- Реферальный трафик из соцсетей также сильно упал, сайты Google дают издателям в два раза больше реферального трафика
- Шеринг контента в социальных сетях упал из-за растущей конкуренции, роста частного шеринга и изменений алгоритмов Facebook.
- Бренды и издатели получают меньше органического реферального трафика из Facebook и меньше вовлечения с постами в сети
- Произошло резкое падение вирусных постов, которые получали сотни тысяч шеров
- Кликбейт-заголовки и списки стали менее эффективны для вовлечения пользователей
- Объем контента от издателей продолжает расти, а области с новыми темами быстро обрастают контентом
- В этих условиях победителями являются сайты, обладающие прочной репутацией благодаря оригинальному и авторитетному контенту.
- Растет шеринг контентом в LinkedIn и издатели видят на этой платформе постоянный рост вовлечения контентом.

***

5.03.2018
Google создал приложение, способное менять задний фон на видео

В Google начали тестировать новую функцию для Youtube, позволяющую заменить задний фон на видео так же просто, как, например, выбрать фильтр к фотографии в Instagram.

Докладніше

***

6.03.2018
Миллиард пользователей выбрали WeChat

На медиа-брифинге, состоявшемся 5 марта в Пекине, исполнительный директор Tencent Holdings Ма Хуатэн (Ma Huateng) объявил о новом этапном достижении популярного чат-сервиса WeChat. Общее количество его активных пользователей за месяц, составлявшее 980 млн в III квартале 2017 г., в феврале 2018 г., в период празднования Лунного Нового Года, впервые превысило миллиард (Компьютерное Обозрение).

WeChat известно в Китае под названием Weixin и является доминирующим в этой стране чат-приложением, выполняющим также функции социальной сети, платформы мобильных платежей, служб доставки пищи, совместных поездок (ride-hailing) и пр.

В дальнейшем, WeChat может стать неотъемлемым элементом жизни каждого китайца благодаря проекту превращения этого сервиса в официальное средство электронной идентификации. Власти Гуанчжоу, столицы южной приморской провинции Гуандун, в декабре дали старт пилотной программе виртуальных удостоверений личности для зарегистрированных пользователей WeChat. Испытания проводятся в городском районе Наньша, но ещё в этом году будут расширены на всю провинцию, а затем и на страну.

Оператор WeChat, Tencent, превосходит по капитализации рынка компанию Facebook, которая однако остаётся крупнейшей в мире социальной платформой с 2,13 млрд активных пользователей на конец прошлого года. Её чат-приложение WhatsApp тогда же перешагнуло отметку в 1,5 млрд активных пользователей.

***

7.03.2018
В Instagram обнаружили секретную функцию

Один из читателей популярного техноблога TechCrunch поделился с изданием информацией о скрытой функции приложения Instagram. Речь идет о так называемом портретном режиме, полагает ресурс (InternetUA).

Обнаружить пока что не реализованную возможность пользователю удалось после декомпиляции установочного APK-файла Instagram для гаджетов на базе Android. В коде прошивки было обнаружено изображение человека в анфас и подписью «portrait_shutter_icon».

Таким образом, в одной из новых версий Instagram может появиться иконка портретного режима – по всей видимости, вместе с самим режимом. Напомним, что в смартфонах такой режим выделяет человека на фото, делая фон расплывчатым.

Представители Instagram отказались комментировать находку читателя TechCrunch, однако само издание напомнило, что функция обмена Giphy GIF была обнаружена похожим образом, а спустя неделю появилась в Instagram официально.

***

11.03.2018

В Facebook появилось распознавание лиц. Это опасно для вас?

На днях в ленте Facebook появилась новость о том, что социальная сеть внедряет дополнительные возможности для распознавания лиц. Разбираемся, зачем это нужно и не опасно ли это.

Докладніше

***

12.03.2018

Facebook тестирует новую технологию дополненной реальности

Компания Facebook экспериментирует с технологией AR в закрытой бета-версии приложения, связанной с предстоящими фильмами «Ready Player One» и «Wrinkle In Time». Приложение Facebook использует плакат фильма в качестве маркера, поверх которого она выстраивает объемное изображение дополненной реальности. Данная технология в апреле будет добавлена в инструмент AR Studio, открытый для всех разработчиков (InternetUA).

Использование специальных подготовленных маркеров позволило Facebook предлагать гораздо более широкий спектр контента AR, а также увеличить точность их размещения в реальном мире. Это должно избавить нас от неловких моментов, когда стандартная маркерная система ARM не может корректно определить точку размещения виртуальных объектов.

Менеджер по продуктам Facebook Мэтью Симари (Matthew Simari) заявил: «Мы полагаем, что в будущем AR будет повсюду. Он будет интегрирован в скрытый слой практически любых объектов, от плаката фильма, до пачки хлопьев. Сегодня мы используем для его просмотра смартфон, а завтра – очки. В данный момент ваш телефон – это увеличительное стекло, которое позволяет заглянуть сквозь вашу реальность в скрытый слой, где царит волшебство».

***

13.03.2018

Instagram лишился новой функции из-за скандала

Разработчики Instagram отключили интеграцию с сервисом Gifhy, которая позволяла использовать GIF-изображения для оформления фото и видео. Причиной стали расистские «гифки», которые обнаружили администраторы сервиса, пишет The Verge (InternetUA).

Одно из GIF-изображений, которое было доступно для пользователей Instagram, представляло собой «счетчик смертей в результате преступлений темнокожих». Многие пользователи Сети обвинили соцсеть в расизме.

«Такому контенту не место в Instagram. Мы приостановили интеграцию с Gifhy до тех пор, пока ситуация не будет расследована», – заявили представители соцсети. Они подчеркнули: пока в компании не будут уверены, что подобное не повторится, GIF-картинки не вернутся в приложение.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

5.03.2018

HereWeAre: Twitter выпустил гимн в честь женщин во время «Оскара»

Социальная сеть запустила первую ТВ-кампанию во время трансляции церемонии награждения «Оскара» #HereWeAre. В 90-секундном ролике звучит поэма Денис Фроман. В видео представлены женщины от 20 до 82 лет, включая актрису Иссу Рей, сценариста Аву Дюверней, кинорежиссеров Джули Дэш и Дженнифер Бреа. Последние строки в поэме произносит сама Фроман. Ролик использует хэштег, который СМО сети Лесли Берланд создала в январе, чтобы высказаться о недостатке женщин-спикеров на CES в этом году (Marketing Media Review).

***

2.03.2018

«Зрадомога»: як українці в соцмережах реагують на «газовий скандал»

Українські користувачі Facebook і Twitter активно обговорюють рішення російського «Газпрому» зменшити тиск в газотранспортній мережі. Подія викликала бурхливу реакцію в українців і спричинила виникнення нових «мемів» (УНН).

Користувачі пишуть жартівливі вірші та пропонують свої методи виходу з ситуації.

Крім того, українці діляться досвідом іноземців у збереженні ресурсів і популяризують новий український хештег #прикрути. Деякі з українців сприйняли хештег аж занадто буквально.

***

10.03.2018

У Тернополі набирає популярності благодійний флешмоб

У мережі Facebook набирає популярності благодійний флешмоб CITRUS LIFE. Його започаткували для того, щоб зібрати кошти на ультразвуковий скальпель для Тернопільського онкодиспансеру (Місто).

За словами організаторів, за кілька тижнів, флешмоб підтримали більше ніж дві сотні людей із різних міст України та з-за кордону.

***

13.03.2018

Житомирян запрошують долучитися до міжнародного флешмобу #LotsOfSocks

Житомирська міська рада та громадська організація «Діти сонця» запрошують житомирян долучитися до міжнародного флешмобу #LotsOfSocks та висловити підтримку людям із синдромом Дауна (Новини Житомира).

Зробити це просто: придбай яскраві шкарпетки та одягни їх 21 березня.

За словами представників ЖОГО «Діти сонця», цьогоріч асортимент різнокольорових шкарпеток навіть більший, ніж у попередні роки, а кошти від їхнього продажу підуть на придбання книжок, іграшок та матеріалів для розвитку для «сонячних» діток.

«Цього року ми зробили таку чисто символічну ціну – від 47 гривень. Чому саме від 47 гривень? Бо наші дітки мають 47 хромосом. Ми ж, як звичайні люди, маємо 46», – розповідає заступниця голови ЖОГО «Діти сонця» Людмила Рибчинська.

До акції вже долучилися міський голова Сергій Сухомлин, його заступниця Вікторія Краснопір, секретар міської ради Наталія Чиж, керуючий справами Ольга Пашко, головний архітектор Житомира Юрій Безбородов, начальник управління у справах сім'ї, молоді та спорту Ірина Ковальчук, а також депутати Житомирської міської ради.

***

9.03.2018

У Луцьку запустили флешмоб #безмаршрутки

Містян у зв'язку з можливим подорожчанням проїзду в маршрутках закликають мінімум один день в тиждень їздити маршрутним таксі, або ж взагалі відмовитись від користування цим видом громадського транспорту (Район.Луцьк).

Про це у Facebook-групі «Наш Луцьк» написав Андрій Михайлов.

Нагадаємо, що у луцьких маршрутках хочуть підняти вартість проїзду до п'яти гривень.

Автор допису пише, що за правилами гри хоча б в один день тижня – вівторок, слід не користуватись маршрутками, а краще – взагалі перейти на інші види транспорту.

***

9.03.2018

Я думаю, президент зрозумів, що припустився помилки, – співавторка флешмобу #ятобінедорогенька

Не прес-конференції, відповідаючи на запитання журналістки «Детектор Медіа» Марини Баранівської, президент звернувся до неї «дорогенька» (Громадське радіо).

На зв’язку зі студією Громадського радіо – співавторка флешмобу #ятобінедорогенька Ірина Земляна.

Наталя Соколенко: Можливо, це вияв панібратства і зверхнього ставлення до людини, а не сексизм? Чому ви цю ситуацію розцінили як сексизм?

Ірина Земляна: Як на мене, тут дуже тонка грань.Чи не є панібратство сексизмом? Я вважаю, що це і панібратство, і сексизм також, тому що він не розглядав Марину, яка ставила питання, як професіоналку, як журналістку, він її розглядав як якусь «дєвочку», яку можна назвати «дорогенька». Він не розглядав її як людину, якій можна і треба відповідати.

Наталя Соколенко: Ви випустили футболки з написом «ятобінедорогенька». Наскільки вони стали популярними?

Ірина Земляна: Я вчора вже бачила на марші жінок з плакатом «Я тобі не дорогенька». Це звернення не тільки до президента, це звернення до усіх чоловіків, тому що у повсякденному житті вони дозволяють собі багато подібних звернень.

Наталя Соколенко: Політолог Євген Магда висловив сумнів, що президент дізнається, що хтось обурюється. А як ви вважаєте?

Ірина Земляна: Я думаю, він вже про це дізнався. Мені подобається наш президент Петро Порошенко тим, що він дуже добре розуміється на інформаційному полі активістів. Він не один раз збирав зустрічі з лідерами думок Фейсбуку. Я очікую від нього реакції. Він прогресивний, проєвропейський. Я думаю, він зрозумів, що припустився помилки і може її виправити, тому я була б рада, якби він виправлявся і вибачався.

***

8.03.2018

Після флешмобу «Я тобі не дорогенька» Президент більше ніколи не дозволятиме собі фамільярність, – Червак

Петро Порошенко обрав не найкращі слова, звертаючись на прес-конференції до журналіста Ірини Земляної. Тому отримав дуже гідну відповідь, у вигляді флешмобу «Я тобі не дорогенька».

Докладніше

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

28.02.2018

Все о Facebook в Украине: аудитория, реклама и рекламодатели

Компания Gemius проанализировала аудиторию Facebook в Украине, объемы размещенной там видеорекламы, а также главных рекламодателей ресурса.

Докладніше

***

7.03.2018

Компании начинают активно внедрять чат-ботов

Аналитики Gartner составили прогноз по широкому распространению виртуальных клиентских помощников (virtual customer assistant, VCA) или чат-ботов в корпоративном секторе.

Докладніше

***

12.03.2018

Facebook заверила издателей, что причина их неудач не в алгоритме ленты

Выступая на ежегодном мероприятии South by Southwest, которое проходит в Остине, США, глава новостных продуктов Facebook Алекс Хардимен ответила критикам, которые называют новый алгоритм сети главным виновником бед издателей. В ответ на вопрос о digital-издателе Little Things, чей CEO обвинил в закрытии компании новостную ленту Facebook, Хардимен отметила: «есть причины, почему определенные издатели не успешны в Facebook». По ее словам проблемы возникают у издателей в том случае, когда

они нарушают систему. Их контент может вводить в заблуждение, звучать сенсационно, приводить в действие предупреждения рекламных ферм. Данные показали, что изменения алгоритма сильно повлияли на издателей. По данным Chartbeat, реферальный трафик Facebook упал на 15 % до того как вступили в силу последние изменения. Хардимен предложила единственное решение: перестать зависеть Facebook. «Мы может быть важной частью вашей стратегии, но мы не будем вашей бизнес-моделью», – добавила она (Marketing Media Review).

***

12.03.2018
Snap надеется стать прибыльной в этом году

Исполнительный директор Snap Эван Шпигель (Evan Spiegel) выразил надежду на то, что компания станет прибыльной в этом году (InternetUA).

В последнем квартале прошлого года убытки компании составили 350 млн долларов, при этом он стал самым успешным кварталом для компании за всю историю существования. За это время в Snapchat появилось около 9 млн новых пользователей. Ежедневная пользовательская база Snapchat по состоянию на конец 2017 года составляла 187 млн человек.

Стать прибыльной компания может, по предположению специалистов, за счет агрессивного снижения затрат и сокращения штата. В сентябре прошлого года Snap уже провела два крупных сокращения, но не планирует останавливаться на этом. Как сообщают хорошо осведомленные информаторы, в ближайшие недели своих рабочих мест лишатся около 120 разработчиков программного обеспечения.

При этом большинство аналитиков считает, что стать прибыльной у компании может получиться не раньше 2021 года.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

6.03.2018
Блогер розповіла про плачевні наслідки «показухи» у соцмережах

Instagram-блогер Ліссетт Кальвейро зі США розповіла, як влізла у величезні борги через постійне бажання публікувати гламурні знімки (Інфотаб).

За словами жінки, їй вдавалося створювати ілюзію розкішного життя у соцмережах, оскільки вона витрачала на це значні суми грошей, – повідомляє New York Post.

У той час, як впливові Instagram-канали показують останні тенденції моди та фото з екзотичних канікул, менш заможні користувачі намагаються не відставати, – зазначає видання.

Так, Кальвейро спустила всі заощадження на новий одяг і походи до дорогих ресторанів, щоб створити видимість щасливого життя в Instagram.

Через кілька місяців борг Кальвейро становив 10 тисяч доларів, проте, вона не могла зупинитися і продовжувала ходити по бутіках і дорогим закладам.

Щомісяця жінка витрачала мінімум 200 доларів на шопінг, щоб не фотографуватися в одному і тому ж одязі двічі. Також їй доводилося купувала хоча б один дизайнерський предмет гардеробу: наприклад, вінтажну сумку Louis Vuitton за тисячу доларів або дорогий аксесуар від Kate Spad.

Зрештою, після переїзду в інше місто, блогер змогла перебороти своє прагнення до створення фейкового іміджу такою ціною.

***

13.03.2018
Соцмережі: вільний обмін думками чи згубна звичка
Громика Наталія

Про невидимі загрози віртуального світу, інтернет-ширму, за якою мільйони користувачів приховують своє справжнє «я», лайки як гормон росту самооцінки і про те, як не стати заручником образу, створеного онлайн та чому корисно мати власні сторінки у соцмережах розповіла психолог-психотерапевт, кандидат психологічних наук, доцент кафедри практичної психології Сумського державного педагогічного університету ім. А. С. Макаренка Дар'я Черенщикова.

Докладніше

***

13.03.2018
Ученые нашли в смартфонах неожиданную опасность для здоровья

Ученые выяснили, что смартфон может вызвать проблемы с психикой у своего владельца. Постоянные звонки и оповещения подталкивают гормоны стресса к действию, постоянно вызывая защитную реакцию «бей или беги».

Докладніше

***

13.03.2018
Запостить за 60 секунд: что происходит в изменчивом мире соцсетей

Статистический портал Statista подсчитал среднее количество действий, которые совершают люди в интернете за одну минуту (Телекритика).

Цифровой мир – это быстро движущаяся и расширяющаяся вселенная со своими правилами и законами. Так, за минуту пользователи успевают отправить 29 миллионов сообщений в WhatsApp, опубликовать 65 тысяч фотографий в Instagram, ввести 3,8 миллиона запросов в Google, отправить более 350 тысяч сообщений в Twitter или залить более 400 часов видео на YouTube.

Портал Statista каждый год выкладывает в свободный доступ актуальную статистику из мира диджитала. Почти все показатели растут ежемесячно. Например, с августа количество поисковых запросов за 60 секунд в Google увеличилось на 0,3 миллиона, а количество публикуемых фотографий в Instagram на 8,5 тысяч. Неизменным осталось лишь количество отправленных электронных писем – 156 миллионов. При этом уменьшилось число твитов – с 452 тысяч до 350 тысяч.

По данным портала, Facebook продолжает доминировать и считается самой популярной соцсетью с двумя миллиардами активных пользователей.

***

13.03.2018

Британский hr-менеджер рассказала, как должен выглядеть ваш профиль в соцсетях

При поиске новой работы не забудьте заглянуть в свои профили в социальных сетях. Британский hr-менеджер рассказала изданию Daily Mail о том, почему профиль кандидата может стать решающим фактором при приеме на работу и как заставить соцсети работать на вас, а не против вас.

Докладніше

Маніпулятивні технології

1.03.2018

Д. Золотухін: Пріоритетним напрямом протидії фейкам є просування власного наративу

27 лютого 2018 року заступник Міністра інформаційної політики України Дмитро Золотухін взяв участь в експертних обговореннях щодо протидії фейковим новинам і дезінформації онлайн, організованих Комісаром ЄС з цифрової економіки та суспільства М. Габріель (Міністерство інформаційної політики).

Дмитро Золотухін представив офіційну позицію Міністерства щодо протидії інформаційним загрозам: «Можливості нормативного регулювання

інформаційного простору для протидії «фейковим новинам» малоефективні через поліморфність, гнучкість і багатогранність дезінформації. Необхідність застосовувати суб'єктивний (а часом і креативний) підхід в оцінці інформації та визначенні фейку створює ризики зловживань. Тому пріоритетним напрямом протидії фейкам варто визначити просування власного наративу та побудову ефективної та стійкої системи державних стратегічних комунікацій».

За результатами експертних обговорень буде розроблено «policy paper» для політичних структур Європейського Союзу щодо питань протидії загрозам поширення «фейкових новин». Участь у заході взяли представники офіційних органів ЄС та окремих країн, представники громадянського суспільства, представники наукових установ, комерційних організацій, think tanks.

***

2.03.2018

Голова Держкомтелерадіо Олег Наливайко взяв участь у дискусії щодо протидії фейкам

Голова Держкомтелерадіо Олег Наливайко взяв участь у слуханнях «Стопфейк: проблема законодавчого регулювання відповідальності за дифамацію у медіа», які відбулися в Комітеті з питань свободи слова та інформаційної політики Верховної Ради України.

Докладніше

***

12.03.2018

Исследование показало, что поддельные новости распространяются в Twitter быстрее и шире настоящих

В эпоху информатизации распространение новостей стало оружием – с его помощью можно сформировать общественное мнение, направить или отвлечь внимание людей, повлиять на принимаемые ими решения (InternetUA).

Пересылая сообщения в социальных сетях, их участники не утруждают себя критическим анализом полученной информации, а возможность привлечь к этому процессу ботов и за их счет придать тому или иному сообщению значительный вес открывает широкие горизонты для манипуляции сознанием.

Исследование, проведенное в массачусетском технологическом институте, показало, что поддельные новости распространяются в Twitter быстрее и шире, чем настоящие. Чтобы сделать такой вывод, исследователи изучили около 126 000 публикаций, которыми поделились друг с другом примерно 3 млн человек в сети Twitter с 2006 по 2017 год. Как оказалось, вероятность пересылки поддельной новости на 70 % выше.

В последнее время Twitter и другие социальные сети, включая Facebook, испытывают давление со стороны американских законодателей и

международных регуляторов, которые обвиняют их в недостаточных усилиях по предотвращению распространения поддельного контента.

Исследователи отмечают два интересных факта. Во-первых, распространение фальшивых новостей активизировалось в 2012 и 2016 году – на эти годы приходятся выборы президента в США. Во-вторых, к удивлению исследователей, реальные пользователи оказались более активными в распространении таких новостей, чем боты.

Спецслужби і технології «соціального контролю»

1.03.2018

Глава АНБ США пожаловался на отсутствие полномочий для борьбы с «русскими хакерами»

Глава Агентства национальной безопасности США, руководитель американского кибернетического командования адмирал Майкл Роджерс (Michael S. Rogers) заявил перед сенатским комитетом по делам вооруженных сил о нехватке полномочий, необходимых для противостояния возможному вмешательству России в промежуточные выборы в Конгресс США, намеченные на 6 ноября 2018 года. Об этом сообщает издание The Washington Post (InternetUA).

По словам Роджерса, определенные меры в данном направлении предпринимаются, однако их может быть недостаточно. Он также пожаловался, что президент США Дональд Трамп не наделяет его новыми полномочиями для «нанесения удара и предотвращения хакерских операций» заранее.

«Мы не решились противостоять России теми же способами, которые она использует по отношению к нам», – отметил Роджерс.

В ответ на заявления главы АНБ, пресс-секретарь Белого дома Сара Сандерс (Sarah Sanders) подчеркнула, что глава киберкомандования не единственное официальное лицо, которому было поручено противостоять вмешательству России в выборы в Конгресс. «Мы работаем над множеством возможных вариантов», – добавила она.

***

28.02.2018

Майя Яровая

Нацполиция предлагает блокировать сайты, ссылаясь на европейские нормы. Что с этим не так

На украинском рынке телекоммуникаций обсуждают очередной законопроект, в котором под видом европейских норм продвигают совсем не европейские практики – в частности блокировку сайтов. Изначальная редакция

закона вызвала много замечаний, однако несмотря на усилия участников рынка, в новой редакции они не были учтены.

Докладніше

***

1.03.2018

«Google не одобряет». Изменения в поиске разозлили пользователей

Сайт Google запретил пользователям из Соединенных Штатов искать товары, в названии которых встречается gun («оружие»), в разделе Shopping. В результате под запрет попали совершенно безобидные товары, что стало причиной для массовой критики сервиса (InternetUA).

«Google теперь блокирует все поисковые запросы со словом gun, и это является проблемой», – написала женщина, которая искала клеевой пистолет.

Под странным запретом оказались даже музыкальные альбомы вроде «Revolver» The Beatles, а также целая группа Sex Pistols.

«Любите британский рок? Google не одобряет».

В Twitter даже появился хэштег #GoogleGunBan. Им помечаются записи, авторы которых жалуются на неприятные изменения в работе поиска Google. Например, купить сигнальный пистолет также не представляется возможным.

Запрет на поиск оружия был принят вскоре после инцидента со стрельбой в школе во Флориде. В Google принесли извинения пользователям и заявили, что работают над устранением ошибки.

***

6.03.2018

Еврокомиссия потребовала удалять террористический контент из соцсетей в течение часа

Европейская комиссия опубликовала новые правила для социальных сетей, согласно которым они должны удалять террористический контент не более чем через час после того, как о нём станет известно.

Докладніше

***

9.03.2018

Трампу разрешили блокировать подписчиков в соцсетях

Американское правительство выступило с заявлением, что блокировка пользователей в личном аккаунте президента США является законной и не противоречит конституции. Об этом сообщает агентство Bloomberg (InternetUA).

Судебные слушания по делу об ограничении доступа некоторых подписчиков к Twitter-аккаунту Трампа прошли 8 марта. По мнению адвокатов,

представляющих правительство, микроблог президента может быть платформой для его официальных заявлений, но блокировка пользователей – это его личное дело.

Судебное разбирательство началось из-за иска Института первой поправки имени Найта Колумбийского университета США. Организация подала в суд на президента и некоторых сотрудников его администрации от имени семи пользователей, заблокированных в официальном Twitter-аккаунте Трампа, которые посчитали, что ограничение доступа и невозможность комментирования заявлений президента наравне с прочими подписчиками нарушает право на свободу слова.

Во время заседания помощник генерального прокурора США Майкл Баэр (Michael H. Baer) призвал окружного судью Наоми Райс Бухвальд (Naomi Reice Buchwald) выбросить иск. По его мнению, любой чиновник имеет право выбора собеседника в интернете. По окончании слушаний Бухвальд призвала стороны разрешить конфликт во внесудебном порядке, а также посоветовала президенту «мьютить» пользователей вместо блокировки.

***

11.03.2018

ФБР настаивает на том, чтобы Google запретил рекламу криптовалютных проектов

Решение Facebook запретить рекламу криптовалютных проектов в прошлом месяце, по-видимому, было не внутренним решением компании, а произошло с подачи ФБР и других регулирующих органов, которые сейчас оказывают аналогичное давление на Google (InternetUA).

Джейсон Рой, старший следователь Комиссии по ценным бумагам Манитобы и председатель рабочей группы по бинарным опционам Канады, заявил:

– Случилось так, что рабочая группа по бинарным опционам Канады, а также ФБР рассказали Facebook о том, что у них вызывает беспокойство, тот факт, что в результате этой рекламы могут пострадать люди.

Мы провели аналогичные беседы с представителями Google и ожидаем от них подобных действий.

Давление на Facebook продолжалось в течение нескольких месяцев. По-видимому, в течение всего этого времени продолжается давление и на Google.

Рой так прокомментировал желание ФБР запретить рекламу ICO и криптовалютных проектов, несмотря на то, что среди них есть много вполне серьезных проектов:

– Вокруг ICO проектов поднялось столько хайпа, что люди просто стали нести туда деньги не заботясь о том, чтобы хоть как-то проверить их или обезопасить свои инвестиции.

Очевидно, что Facebook предпочел последовать «совету» ФБР и прекратить рекламу ICO и криптовалютных проектов, хотя их юридический

статус во многом остается неопределенным. Поддастся ли Google на давление нам еще предстоит увидеть.

Проблема захисту даних. DDOS та вірусні атаки

28.02.2018

Волинянин розповсюджував мобільний додаток, який «краде» гроші з рахунків

Історія про те, як двоє вмілих та перспективних студента вирішили нелегально підзаробити. Маючи навички програмування, вони розробили власний мобільний додаток, за допомогою якого отримували доступ до банківських рахунків користувачів мобільного банкінгу.

Докладніше

***

28.02.2018

Уязвимость в Facebook раскрывала данные администраторов страниц

Исследователь кибербезопасности из компании Seekurity Мохамед Басет (Mohamed Baset) обнаружил в социальной сети Facebook уязвимость раскрытия информации, позволяющую просматривать имена и другие данные администраторов страницы (InternetUA).

По словам исследователя, проблема была выявлена после того, как на его почту пришло сообщение с предложением поставить отметку «Нравится» странице, на которой он ранее отметил понравившейся отдельную публикацию. Проанализировав исходный код полученного письма, эксперт заметил, что оно включает имя администратора страницы и другие сведения.

Басет уведомил Facebook об уязвимости, после чего компания выплатила ему $2,5 тыс. вознаграждения, а проблема была исправлена.

Исследователь безопасности из компании Sophos Пол Даклин (Paul Ducklin) объяснил, почему подобные уязвимости раскрытия информации могут представлять проблему для администраторов страниц Facebook.

«Для бизнес-страниц или сообществ, в которых может быть несколько администраторов, Facebook не должна раскрывать ничего, кроме имени самой страницы, по крайней мере без разрешения. Это защищает отдельных сотрудников от получения множества комментариев и вопросов», – отметил эксперт.

В общей сложности в прошлом году Facebook выплатила исследователям более $800 тыс. за обнаруженные уязвимости.

***

28.02.2018

Российских хакеров подозревают во взломе сети правительства ФРГ

В Германии хакерскую атаку обнаружили в декабре прошлого года. Эксперты не исключают, что она длилась в течение всего прошлого года (InternetUA).

Российские хакеры взломали компьютерную сеть правительства Германии. Хакерская группа APT28 смогла проникнуть в сеть министерств иностранных дел и обороны, 28 февраля агентство dpa со ссылкой на источники в немецких спецслужбах. По их данным, хакеры внедрили в сеть вредоносные программы и похитили документы. Немецкие спецслужбы обнаружили атаку в декабре 2017 года, эксперты не исключают, что она длилась в течение всего прошлого года.

Специалисты пытаются выяснить, насколько глубоко хакерам удалось проникнуть в правительственную сеть, которой пользуются ведомство федерального канцлера, федеральные министерства, ведомство по уголовным делам, счетная палата, а также спецслужбы.

Группе APT28, известной также под названием Fancy Bear, приписывают также нападение на внутреннюю сеть бундестага в 2015 году, в ходе которого они скачали порядка 17 гигабайт данных. Специалисты считают, что APT28 работает под руководством Главного разведуправления (ГРУ) вооруженных сил России.

***

28.02.2018

Хакеры активно эксплуатируют уязвимость в Adobe Flash Player

В начале февраля нынешнего года мы сообщили о новой критической уязвимости нулевого дня в Adobe Flash Player (CVE-2018-4878), активно эксплуатируемой хакерской группировкой APT37 (также известна как Reaper, Group123 и ScarCruft) в атаках против Южной Кореи. Хотя Adobe выпустила корректирующее обновление Flash Player 28.0.0.161 спустя несколько дней после обнародования информации о проблеме, многие компании по-прежнему используют уязвимую версию продукта, чем и пользуются киберпреступники (InternetUA).

В ходе кампании злоумышленники распространяют спам-сообщения, содержащие ссылку на документ Microsoft Word, расположенный на ресурсе storage[.]biz. Для просмотра контента загруженного документа жертве рекомендуется включить режим редактирования. Если пользователь следует инструкции, вредоносный шелл-код запускает командную строку и подключается к домену атакующего. Затем на устройство загружается и с помощью утилиты Microsoft Register Server (regsvr32) исполняется DLL-библиотека.

Вредоносные письма включали несколько коротких ссылок, созданных с помощью сервиса Google URL Shortener. По оценкам исследователей, за 3-4 дня кампании переход по этим ссылкам осуществлялся десятки и сотни раз.

«Как и ожидалось, злоумышленники быстро взяли на вооружение эксплоит для уязвимости в Adobe Flash Player. Слегка изменив атаку, они успешно запустили масштабную вредоносную кампанию и в очередной раз обошли большинство существующих статических сканеров», – отметил эксперт Morphisec Labs Майкл Горелик (Michael Gorelik).

***

1.03.2018

Самое мощное интернет-оружие сделали еще опаснее

Эксперты по безопасности из компании Fortinet рассказали об обновленной версии крупнейшего в мире ботнета Mirai. Об этом сообщается на официальном сайте компании (InternetUA).

Специалисты прозвали модификацию червя Mirai OMG. В отличие от предыдущей версии, новый ботнет не только использует уязвимости интернета вещей, но и превращает IoT-устройство в прокси-сервер. Благодаря этому, злоумышленники получили возможность пропускать через зараженные девайсы вредоносный трафик. Это позволит хакерам лучше скрывать местоположение, а также осуществлять более мощные атаки.

Впервые о ботнете Mirai заговорили в середине 2016 года. Разработчики ботнета атаковали сайт эксперта по интернет-безопасности Брайана Кребса: объем трафика достигал 660 гигабайт в секунду. Тогда специалист назвал ботнет «мощнейшим оружием современности».

Спустя полгода сотрудники ФБР вычислили создателей Mirai: ими оказались американские студенты Далтон Норман, Парас Джа и Джозая Уайт. По словам молодых людей, они хотели подзаработать на своей идее: студенты устраивали DDoS-атаки на чужие серверы компьютерной игры Minecraft, переманивая при этом игроков на собственные серверы. Однако когда подростки увидели всю мощь созданного ботнета, они опубликовали исходный код Mirai в сети, чтобы другие хакеры также могли его использовать. В итоге под DDoS-атаками рухнуло множество крупных ресурсов, среди которых оказались GitHub, Spotify, Twitter и Reddit.

***

1.03.2018

Пользователям советуют срочно удалить популярное приложение

Изначально приложение GetContact разрабатывали как блокировщик SMS-рассылок и нежелательных звонков. А потом разработчики решили пересмотреть функциональность программы и добавили любопытную фичу.

GetContact позволяет узнать, как ваши близкие и друзья записали вас в свою телефонную книгу.

Докладніше

***

5.03.2018

Киберпреступники все больше фокусируются на целевых атаках

Аналитическая информация компании Trend Micro за 2017 г. показывает, что программы-вымогатели продолжали атаковать организации по всему миру наряду с всплеском скрытого майнинга криптовалют. Эти тенденции продолжат развиваться в 2018 г., а вымогательство, вероятно, будет нацелено на организации, пытающиеся соответствовать новым законам конфиденциальности «Общего регламента по защите данных» (GDPR, General Data Protection Regulation) (Компьютерное Обозрение).

Новый отчет «Парадокс киберугроз» (The Paradox of Cyberthreats) подтверждает прогнозы Trend Micro на 2018 г. – преступники все чаще отказываются от использования эксплойтов и беспорядочных нападений в пользу стратегических атак, направленных, в первую очередь, на финансовую выгоду. Вполне вероятно, что злоумышленники по-новому подойдут к вымогательству: они определят размер штрафа в рамках GDPR, который компания должна будет заплатить в результате атаки, и потребуют выкуп, который обойдется руководству в меньшую сумму.

Количество программ-вымогателей увеличилось на 32 % за период с 2016 по 2017 гг. Число BEC-атак во второй половине прошлого года вдвое превысило показатели первых шести месяцев. По прогнозам экспертов Trend Micro, потери от таких атак превысят 9 млрд долл. в 2018 г.

Темпы разработки вредоносных программ для майнинга криптовалют постоянно растут – в октябре было обнаружено 100 тыс. программ. Устройства Интернета вещей (IoT) также подвержены риску. Решения Trend Micro обнаружили 45,6 млн случаев скрытого майнинга, которые составляют большую часть от всех обнаруженных инцидентов, связанных с Интернетом вещей.

***

5.03.2018

28 февраля произошла крупнейшая в истории DDoS-атака

В последний день февраля хостинговый сервис для исходных кодов GitHub подвергся самой крупной DDoS-атаке за всю историю интернета. Как сообщают администраторы сайта, злоумышленники перехватили IP-адреса GitHub и контролировали систему распределения памяти ресурса. Таким образом хакеры генерировали трафик со скоростью 1,35 терабита в секунду, из-

за чего серверы GitHub некорректно работали в течение нескольких минут. Владельцы сервиса рассказали, как им удалось остановить атаку (IGate).

Количество трафика GitHub резко увеличилось во время атаки, из-за чего сайт полностью отключился на несколько минут

Отразить атаку на GitHub помогли центры Akamai Prolexic. Серверы посредника маршрутизировали входящий и исходящий трафик с GitHub. Спустя восемь минут вредоносные пакеты были отсеяны, и сайт вернулся в стандартный режим.

Напомним, портал уже становился мишенью хакеров в 2015 году. Тогда злоумышленники атаковали ресурс в течение пяти дней.

***

5.03.2018

Що про вас знає Facebook, навіть якщо його у вас немає. 38 фактів

Facebook може відслідковувати ваші рухи онлайн, навіть якщо ви ніколи не відвідували сайт цієї соціальної мережі. Про те, що найбільша соціальна мережа у світі створює секретні файли про діяльність мільярдів людей, пише The Daily Mail.

Докладніше

***

5.03.2018

Майя Яровая

В интернете появились фейковые сайты Monobank, которые выманивают деньги и данные

В уанете появились мошеннические сайты, которые маскируются под Monobank. Один из них выманивает у пользователей пароли и SMS от банка – таким образом мошенники пытаются заменить смартфон клиента на свой и получить доступ к его деньгам. Вторая схема: пользователям сообщают, что Monobank якобы выпустили версию для десктопа, и предлагают клиентам пройти регистрацию. Об этом сообщил сооснователь Fintech Band Олег Гороховский (AIN.UA).

Сайт размещается на незащищенном домене, однако от настоящего его не отличить – дизайн практически идентичный.

«Это мошенники. Мы не планируем делать версию для десктопов и любые подобные сообщения просто отправляйте в спам. Также мы нигде не просим вводить ПИН, а SMS-код клиент Monobank вводит всего один раз, когда регистрируется в приложении», – подчеркивает Гороховский.

Он также заявил, что украсть данные клиентов мобильного банка сложнее, чем десктопного. Именно поэтому Fintech Band изначально сосредоточилась исключительно на смартфонах. «Мы реализовали систему, в которой есть жесткая связка IMEI устройства, ID версии приложения,

установленной у клиента, номера телефона и пина и если хоть один параметр не совпадает – это фрод. И такую связку практически невозможно взломать и главное в ней это конечно же IMEI», – подчеркнул Гороховский.

***

5.03.2018

1+1 медіа запускає комерційний проект для захисту авторських прав в інтернеті

Група «1+1 медіа» оголосила про запуск нового комерційного продукту SUDUM – технологічно-правової системи для захисту авторських прав в інтернеті, яка допомагає блокувати нелегальні копії відеоконтенту на сайтах, популярних соціальних мережах та відеохостингах.

Докладніше

***

6.03.2018

Россия использует Украину, как тестовую площадку для кибератак – МВД Великобритании

Главы МВД Украины и Великобритании Арсен Аваков и Бен Уоллс на встрече обсудили планы по совместной отработке механизма борьбы с киберпреступностью и организованной преступностью между странами.

Докладніше

***

6.03.2018

Зафиксирована первая «настоящая» DDoS IPv6 атака

Сеть DNS-службы Neustar стала жертвой первой зафиксированной «настоящей» IPv6 DDoS-атаки. Источниками «атаки по словарю» являются порядка 1,9 тыс. узлов IPv6, принадлежащих к более чем 650 сетям. Об этом сообщило издание SC Magazine UK (InternetUA).

По словам представителей Neustar, данная атака примечательна тем, что злоумышленники используют новые методы вместо копирования уже существующих, однако с применением IPv4. Атаки IPv6 могут причинить серьезный вред, например, превысить объемы памяти современных средств безопасности за счет большого количества адресов, доступных хакерам.

В общей сложности IPv6 содержит более чем в 7.9×1028 раз больше адресов чем IPv4, который использует 32-битные адреса и позволяет организовать порядка 4,3 млрд адресов. Таким образом количество потенциальных атак также вырастает в разы. При этом, множество сетей, поддерживающих протокол IPv6, не поддерживают инструменты для противодействия хакерам.

Как отметили специалисты, в текущем году наблюдается значительный рост количества IPv4 атак – оно удвоилось в сравнении с аналогичным периодом 2017 года.

Neustar – технологическая компания, которая предоставляет информацию и аналитику в реальном времени для интернет-индустрии, телекоммуникаций, развлечений и маркетинга, а также предлагает услуги обмена информацией для глобальных коммуникаций.

***

7.03.2018

Найден способ читать чужую переписку пользователей популярной соцсети

Сторонний программист обнаружил уязвимость в соцсети «ВКонтакте», позволяющую читать переписку пользователей. Об этом сообщает портал TJ (InternetUA).

Анонимный SEO-разработчик Yoga2016 использовал сервис по получению статистики сайтов и соцсетей из поисковиков SimilarWeb. Он обнаружил, что если через платную версию программы проанализировать «Вконтакте», то, как и в случае с другими сайтами, можно просмотреть 300 самых материалов конкретного сайта, коими в случае соцсети оказались страницы пользователей.

Уточняется, что таким образом нельзя попасть на страницу какого-либо определенного пользователя, SimilarWeb предлагает для анализа случайную выборку «популярных» страниц, при этом критерии отбора неясны – у ряда аккаунтов по 50 друзей и слабая активность.

Разработчик рассказал, что обратился во «ВКонтакте» в рамках программы Bug Bounty, однако обещанного вознаграждения за выявленную ошибку не получил. В пресс-службе «ВКонтакте» пояснили, что уязвимость не связана с проблемой соцсети, а создана разработчиками, которые имеют доступ к API (интерфейс прикладного программирования). К примеру, они могут использовать личную переписку в альтернативных клиентах для мессенджера «ВКонтакте» с разрешения пользователей.

***

7.03.2018

В сетях 4G LTE есть уязвимость, позволяющая следить за пользователями

Во многих странах мира пользователям доступны мобильные сети четвертого поколения, которые поддерживаются основной частью мобильных девайсов (iLenta.com).

Как оказалось, в сетях 4G LTE есть уязвимость. Ее обнаружили специалисты из университетов Айовы и Пердью. Они смогли найти десять типов атак на сети 4G LTE.

Уязвимости касаются трёх основополагающих операций сотовых сетей – безопасного подключения устройства к сети, поддержание соединения для получения звонков и сообщений.

Указанные атаки, в случае использования, позволяют злоумышленникам следить за пользователями, отслеживать их местоположение, читать сообщения и прослушивать звонки.

Атаки позволяют создать «искусственный хаос», распространяя ложные сообщения о чрезвычайных ситуациях абонентам в определённой местности для отвлечения внимания.

***

10.03.2018

Хакери під час атаки на МЗС Німеччини викрали документи щодо України і Brexit

Пов’язані з Росією хакери, що вчинили атаку на німецькі урядові сайти, викрали документи, які стосувалися переговорів щодо виходу Британії з ЄС (Brexit), України і Білорусі, повідомила «Європейська правда» з посиланням на Spiegel Online (InternetUA).

Всього хакерам вдалося викрасти шість файлів. Серед них документ, який стосувався переговорів між Британією і ЄС щодо Brexit, а також переговорів з Україною та Білоруссю.

Як зазначається, витік документів щодо України і Білорусі стався, коли служба безпеки вже дізналася про атаку і контролювала її перебіг.

Як стало відомо 28 лютого, хакерська група APT28, яку зазвичай пов’язують з Росією, атакувала сервери МЗС і Міноборони Німеччини.

Хакерська група APT28, також відома як Fancy Bears, здійснює кібератаки на державні, інформаційні, військові та інші структури країн. Групу підозрюють, зокрема, в здійсненні масштабної атаки на внутрішню мережу німецького парламенту в травні 2015 року.

***

11.03.2018

Apple угрожает выложить все данные в сеть при попытке удалить аккаунт

Один из китайских пользователей приложения Apple iCloud пожелал отказаться от услуг Apple, после того, как власти КНР приняли закон о хранении личных данных юзеров только в Китае. Мужчина обратился в службу технической поддержки и вместо того, чтобы выполнить просьбу пользователя, сотрудник начал угрожать и шантажировать клиента (InternetUA).

Когда клиент обратился к сотруднику корпорации с просьбой об удалении аккаунта, то работник попытался уговорить юзера не удалять учетную запись. Однако клиент оказался настойчивым и продолжал стоять на своем. Тогда сотрудник Apple узнал у владельца смартфона данные учетной записи, авторизировался и стал шантажировать китайца.

На данный момент пока неизвестно, был ли этот инцидент самоуправством одного из работников «яблочной» корпорации или же это политика у Apple такая. Но пользователи Apple ID все же должны задуматься.

***

12.03.2018
Роман Черный
Киберпреступники натравят на вас искусственный интеллект

Представьте себе следующую ситуацию. Вы получаете звонок или голосовое сообщение от близкого человека, который сейчас путешествует за границей. Он утверждает, что потерял телефон и деньги и просит вас о помощи. Ранее вы получали электронные письма с подобными просьбами, но, будучи технически подкованным человеком, решили, что вас пытаются «развести». Но на этот раз никаких сомнений нет – вы собственными ушами слышите голос своего знакомого. Вы переводите деньги. И напрасно. Ведь этот голос сгенерирован при помощи искусственного интеллекта. Из соцсетей преступники получили все необходимые сведения, включая образцы голоса потенциальной жертвы. Затем – сформировали соответствующие голосовые сэмплы при помощи интеллектуального алгоритма.

Докладніше

***

12.03.2018
Через соцсети хакеры получают личные данные чаще, чем через порносайты

Часто хакеры на ресурсах с откровенным контентом размещают вредоносные программы с целью получения доступа к конфиденциальной информации юзеров. По мнению экспертов, в плане потери личных данных более опасными являются социальные сети, чем порносайты (InternetUA).

Летом 2017 года 17-летний парень из Мончегорска обнаружил критическую уязвимость во «ВКонтакте». Юный хакер получил доступ к любому аккаунту без двухфакторного кода. Представители ресурса сообщали, что утечка произошла с 400 тысяч страниц юзеров. Благодаря стороннему приложению кибермошенник проник в систему и взломал аккаунты. В Сети появилась конфиденциальная информация со страниц, которые отобрали по случайному принципу.

Вредоносная программа определяет поисковые запросы и браузеры пользователей. Администрация социальной сети «ВКонтакте» отреагировала на сообщение о мошенничестве. Технические специалисты устранили ряд проблем и лишили хакеров возможности получать личные данные юзеров, надолго ли хватит новой защиты покажет время.

***

12.03.2018

Уязвимости в Facebook раскрывали списки друзей и платежные данные

Исследователь безопасности Йосип Франькович (Josip Franjković) обнаружил в приложении Facebook для Android уязвимости, позволяющие получить доступ к списку друзей пользователей соцсети и узнать их платежные данные.

Докладніше

***

12.03.2018
Юри Кострубати
Хакеры заражают ПК для заработка криптовалюты

Специалисты «Лаборатории Касперского» обнаружили хакерские группировки, использующие методы и техники сложных целевых атак для распространения троянов, предназначенных для скрытой добычи криптовалюты (IT новости).

Бум цифровой валюты привел к тому, что пользователи интернета все чаще подвергаются атакам программ-Майнеров.

По оценкам, частота таких нападений в прошлом году выросла практически в полтора раза по сравнению с 2016 годом.

Для распространения вредоносных программ с функциями добычи цифровой валюты используются различные методы. Такие трояны могут прятаться в различных приложениях или играх. Пользователи становятся жертвами рекламного ПО.

Кроме этого, мошенники начали прибегать к сложным техникам заражения – целевым атакам. Схема нападений выглядит так. Жертву заставляют скачать и установить ПО, скрытый Майнер. Программа работает как утилита для Windows, а его основная цель – скачать сам майнер с удаленного сервера. После запуска приложения запускается легитимный процесс, а его код меняется на вредоносный.

В результате вирус работает под прикрытием легитимного процесса, поэтому пользователь не может распознать заражения. Хакеры делают так, что отменить задачу становится невозможно: при попытке остановить операцию

система перезагружается. В результате преступники обеспечивают свое присутствие на компьютере на длительное время.

***

13.03.2018

Скрытый майнинг: хакеры атаковали компьютеры в России, Украине и Турции

Более 400 тысяч персональных компьютеров были атакованы в рамках попытки распространения вредоносного ПО для майнинга криптовалют. Хакеры использовали сложные трояны для заражения ПК в основном в России, но также в Турции, Украине и других странах.

Докладніше

ДОДАТКИ

Додаток 1

28.02.2018

Viber запускає нову функцію – глобальні спільноти, які можна монетизувати

Месенджер Viber презентував нову функцію «спільноти» – сервіс для обміну повідомленнями в форматі групового чату, при цьому адміністратори отримують нові опції для модерації дискусії (Watcher).

Адміністратори спільнот отримають можливість формувати групи однодумців на основі спільних інтересів та інших факторів. У прес-службі Viber також повідомили Watcher про те, що незабаром Viber представить нові функції для монетизації, за допомогою яких, власники спільнот зможуть отримувати прибуток, розвиваючи свої чати.

Нові учасники отримають доступ до повної історії чату та одразу після реєстрації зможуть взяти участь в обговоренні. У спільнотах будуть відображені тільки імена користувачів, а номери телефонів та інша особиста інформація – приховані від інших учасників.

Суперадміністратори повністю контролюватимуть діяльність спільнот. Вони зможуть додавати нових учасників, надавати їм статус адміністратора або суперадміністратора, блокувати користувачів за некоректний контент, давати дозвіл на участь в обговореннях і право запрошувати нових учасників. Для просування своєї спільноти, модератори зможуть зробити її загальнодоступною. Вони просто активують можливість переходу за посиланням, або в будь-який момент відключать цю опцію.

Суперадміністратори зможуть призначати адміністраторів для допомоги в модерації спільноти з правом видалення одного або всіх повідомлень, відправлених тим чи іншим учасником, а також з правом закріплення обговорюваних повідомлень. Адмінам буде надана можливість розвивати

спільноту, додаючи нових учасників і, при необхідності, виключати з неї користувачів.

Новий функціонал вже використовує французький футбольний клуб Olympique de Marseille, і надає фанатам ексклюзивний шанс поспілкуватися із зірками та керівниками команди. Компанія Minute Media, що спеціалізується на створенні та розповсюдженні спортивного контенту, використовує спільноти Viber, для обміну думками між шанувальникам спорту. Служба цифрового контента OverDrive приєдналася до онлайн спільнот для пошуку книжкових клубів, створених громадськими бібліотеками в США.

(вгору)

Додаток 2

28.02.2018

Дмитрий Демченко

Что такое Vero – социальная сеть, которую называют убийцей Instagram

Последние несколько дней в западных СМИ активно обсуждают социальную сеть Vero, которая неожиданно набрала большую популярность. Создатели называют ее самой «аутентичной», а некоторые западные СМИ уже окрестили сервис «убийцей» Instagram. Редакция AIN.UA рассказывает, что известно о социальной сети (AIN.UA).

Vero была запущена в 2015 году, но популярность набрала только в феврале 2018-го.Основатель сервиса – ливанский миллиардер и предприниматель Айман Харири. Он говорит, что идея Vero к нему пришла из-за «разочарования во всех существующих социальных сетях».

За последнюю неделю Vero поднялась на высшие строчки в американских App Store и Google Play в категории «Бесплатные приложения», а также вышла на показатель в 500 000 загрузок в день суммарно на iOS и Android. Для сравнения – до этого за все время существования сервиса приложения скачали всего 600 000 раз. В Vero объясняют такую популярность тем, что в социальную сеть начали мигрировать участники тату и косплей-сообществ. В Instagram, например, сейчас насчитывается более 500 000 публикаций с хештегом #vero.

Главные особенности Vero – хронологическая лента и отсутствие рекламы. Как отмечает Харири, отсутствие рекламы – принципиальное отличие Vero от других сервисов. Другая особенность, на которую активно обращают внимание создатели, – минимальное количество данных, которые сервис собирает о пользователях.

Во всем остальном социальная сеть работает по аналогии с Instagram и Facebook. Здесь можно публиковать фото, видео, ссылки, отзывы о книгах, фильмах и сериалах, а также делиться местоположением. Пользователь может добавлять друзей и общаться с ними в чатах. Одна из «фич» Vero – возможность указывать уровень отношений с людьми в сервисе (близкие

друзья, друзья, знакомые и подписчики) и публиковать записи только для определенной группы.

Vero уже заключила партнерство с известными брендами (британский GQ) и знаменитостями, среди которых певица Charlie XCX и режиссер Зак Снайдер. Они предоставляют эксклюзивный контент для социальной сети.

Социальная сеть планирует зарабатывать на подписке. Создатели говорят, что плата будет составлять «несколько долларов» в год. Правда, когда подписка заработает неизвестно – пока что сервисом можно пользоваться бесплатно. Также создатели социальной сети планируют сделать из Vero маркетплейс, где бренды смогут продавать свой товар, а сервис будет брать за это комиссию. Например, в октябре 2016 года через Vero был продан автомобиль Aston Martin за $1 млн.

Несмотря на популярность, многие пользователи уже недовольны социальной сетью. Например, в Twitter люди жалуются на постоянные сбои в работе сервиса. «Приложение очень медленное, вероятно, из-за притока новых пользователей. Ко всему прочему, интерфейс очень запутан», – написал журналист Mashable Брайан Корбер.

Другие СМИ узнали о прошлом основателя Vero Аймара Харири. Издание Daily Beast опубликовало статью, где рассказало, как Харири работал заместителем главы уже не существующей строительной компании Saudi Oger. Во времена его работы компания не выплачивала зарплату более 31000 сотрудникам, из-за чего в ситуацию пришлось вмешаться властям Саудовской Аравии. Эта история также спровоцировала негативные отзывы пользователей.

Daily Beast также обратило внимание, что отдел разработки Vero находится в России: «Множество стартапов отдают разработку на аутсорс, но не все генеральные директора имеют братьев, близких к Путину». Издание имеет в виду брата Аймара Харири, создателя Vero, Саада. Ранее Саад Харири занимал пост премьер-министра Ливана и активно вел переговоры о сотрудничестве с Россией.

(вгору)

Додаток 3

2.03.2018

Facebook закрыла эксперимент с дополнительной лентой новостей

Социальная сеть Facebook объявила об окончании начатого в октябре прошлого года эксперимента, в рамках которого компания тестировала разделение ленты новостей на две разные ленты в нескольких странах мира. Сообщение об этом было опубликовано в блоге Facebook (InternetUA).

В рамках тестирования, проходившего с участием пользователей из Боливии, Гватемалы, Камбоджи, Сербии, Словакии и Шри-Ланки, соцсеть выделила в отдельную ленту под названием Explore записи публичных страниц, оставив в основной ленте публикации друзей и родных. Однако пользователи

не оценили это нововведение, отметив, что наличие двух лент не способствует лучшей коммуникации с друзьями.

«Людям не нужны две разные ленты. Опросы показали, что пользователи с двумя лентами менее удовлетворены, наличие двух отдельных лент не помогало им больше общаться с друзьями или семьей. Пользователи также пожаловались на то, что им стало труднее получать важную информацию и что мы недостаточно ясно изложили суть теста», – приводит VC.ru комментарий вице-президента Facebook Адама Моссери.

В связи с негативными откликами в Facebook приняли решение свернуть эксперимент. Как отмечается в сообщении компании, недавние изменения алгоритмов формирования основной ленты, в результате которых пользователи видят больше записей друзей и меньше публикаций брендов и СМИ, лучше отвечают запросам людей на общение.

(вгору)

Додаток 4

5.03.2018

Google создал приложение, способное менять задний фон на видео

В Google начали тестировать новую функцию для Youtube, позволяющую заменить задний фон на видео так же просто, как, например, выбрать фильтр к фотографии в Instagram. Приложение, созданое с применением алгоритма искусственного интеллекта, способно делать это «на лету», минуя необходимость использовать зелёный экран и прочие сложные приспособления. Инструмент редактирования уже доступен для смартфонов, но пока только в бета-версии и для небольшого круга пользователей (IGate).

Пока функцию тестируют в новом видеоформате «истории», напоминающем одноимённые функции из Snapchat или Instagram. Ниже можно посмотреть пример того, как работает новое AI-приложение.

«При разработке использовалось машинное обучение для решения задачи семантический сегментации с использованием нейронных сетей. Мы создали сетевую архитектуру и учебную процедуру, подходящую для смартфонов. Нам хотелось, чтобы приложение было лёгким и быстрым, поэтому мы изначально поставили себе задачу заставить его работать в 20-30 раз быстрее других современных моделей сегментирования фотографий. Это позволило нам добиться результата, при котором всё это «летает» со скоростью до 30 кадров в секунду», – поясняют специалисты, работающие над приложением.

Результат пока сложно назвать идеальным, но и разработка приложения далека от завершения. Сейчас при выборе тёмных фонов можно заметить небольшие засветы и «нимбы» над головой девушки, демонстрирующей новую функцию. Наверняка к релизу публичной версии алгоритм научится работать аккуратнее, тщательнее обрезая края и подгоняя слоя видеоролика и заднего фона. Будет здорово, если разработчики добавят в утилиту и другие

возможности, например, позволяющие вставлять на задний фон собственные изображения, но это будет известно ближе к релизу.

(вгору)

Додаток 5

11.03.2018

В Facebook появилось распознавание лиц. Это опасно для вас?

На днях в ленте Facebook появилась новость о том, что социальная сеть внедряет дополнительные возможности для распознавания лиц. Разбираемся, зачем это нужно и не опасно ли это (InternetUA).

Как всё работало раньше

Распознавание лиц работает в Facebook с 2010 года. Конечно, с тех пор технология стала куда точнее, но суть не изменилась.

Когда вы загружаете фото, система выделяет лица на них и сравнивает со снимками из своей базы. Естественно, сначала она сравнивает лица на снимках с вашими фото, затем – с фото ваших друзей и т. д. Таким образом, вероятность опознавания увеличивается, а сложность обработки сокращается.

Изначально функция распознавания лиц вводилась, чтобы пользователям было легче отмечать друзей на фото. Социальная сеть сама определяла, кто из друзей попал в кадр, а автор снимка мог согласиться с этим или переотметить людей вручную.

Что за дополнительные возможности ввели

В декабре 2017 года соцсеть стала уведомлять пользователей, если кто-то загружал фото с ними даже без тегов и отметок. Сначала доступ к функции получили жители США, затем она стала распространяться и в другие страны. В конце февраля 2018 года очередь дошла и до России, Украины и ряда других стран.

Функция призвана защитить от кражи личных фотографий. Если кто-то загрузит фото с вами, вы получите уведомление. Можно отклонить отметку на фото, если автор её устанавливал, или попросить его удалить изображение. Руками ничего искать не надо – перейти к фото можно прямо из уведомления.

Кроме того, функция предупредит создание фейковых профилей с вашими фото. Такие профили часто используют злоумышленники – чтобы казаться не тем, кем они являются на самом деле, чтобы выманивать деньги и порочить вашу репутацию.

Как распознать лицо на фото

Для распознавания лиц используется последовательность интеллектуальных алгоритмов. На первом шаге программа пытается понять, есть ли вообще люди на фото, и выделяет овалы лиц.

Затем алгоритм исследует пространство внутри этого овала и выделяет ключевые точки, чтобы указать, где на фото нос, глаза и рот. Эти точки служат ориентирами, которые позволяют развернуть лицо фронтально – как будто человека фотографируют на паспорт.

Далее алгоритм работает уже с преобразованным изображением. Интеллектуальный алгоритм распознавания лиц Facebook измеряет несколько десятков параметров, к примеру, расстояние между глазами, расположение и ширина носа, рта и др.

На основании измерений, проведенных по фото, социальная сеть создаёт шаблон лица. Его просто применять для анализа новых фото. Разработчикам конкретные значения параметров неизвестны, ведь алгоритм фактически получает их в процессе обучения. Параметры сравниваются со значениями из базы, и если находится соответствие, Facebook ставит отметку на фото.

Facebook расскажет, что на фото

Возможности алгоритма распознавания Facebook определяют на фото не только лица, но и другие значимые объекты. Эта возможность призвана помочь слепым и слабовидящим людям пользоваться социальной сетью. В итоге каждый человек может получить описание объектов на фото и имена людей, которые, скорее всего, изображены на снимке (но они при этом не тегаются).

Юридический вопрос

Федеральный судья Джеймс Донато заявил, что социальная сеть «должна столкнуться с утверждениями о том, что она нарушает конфиденциальность миллионов пользователей путем сбора и хранения биометрических данных без их согласия». Так, Facebook нарушает закон штата Иллинойс и потенциально должна платить от 1 до 5 тыс. долларов каждый раз, когда изображение человека используется без разрешения.

Первые иски от пользователей из штата Иллинойс по поводу незаконного распознавания лиц были поданы в адрес Facebook ещё в 2016 году. Но тогда Facebook заявлял, что истцам не был нанесён конкретный ущерб: физический вред, потеря денег или имущества, отказ в праве на свободу слова или вероисповедания.

Донато отклонил аргументы о том, что дело нужно прекратить, так как соблюдение законов штата Иллинойс противоречит пользовательскому соглашению Facebook. Оно требует разрешения споров в соответствии с законодательством Калифорнии, где основана компания.

В общем, судья Донато вынес постановление о том, что будет рассматривать групповой иск в адрес Facebook. Он подчеркнул, что технология распознавания лиц нарушает конфиденциальность пользователей.

Если дело завершится не в пользу Facebook, функцию могут и отключить (и заставить соцсеть заплатить до 5 тыс. долларов за каждое фото). А так как отделить пользователей из Иллинойса от всех остальных сложно, убрать распознавание могут для всех.

Недостатки новой функции

Если снимки защищены настройками приватности, уведомления вы не получите. Значит ли это, что кто-то может выкладывать снимки с последнего корпоратива в закрытое сообщество или только для друзей, в число которых вы не входите? Да, и ему за это ничего не будет. А вы ничего об этом не узнаете. По крайней мере, от Facebook.

К тому же функция включена по умолчанию. А значит, Facebook уже создал шаблон вашего лица. И, вероятно, где-то его хранит. Утверждается, что шаблоны удаляются, когда вы отключаете функцию. Но кто знает, кто знает…

К тому же соцсеть заявляет:

Эта настройка отображается в профиле только лиц старше 18 лет и доступна не во всех странах.

А что, если Facebook за нами шпионит

Само наличие функции распознавания лиц говорит о том, что:

1.Facebook может связывать лица на фото с профилями пользователей.

2.Facebook располагает базой данных людей с установленными связями между ними и активно использует её для поиска и т. д.

3.Facebook ничего не стоит распознавать людей на фото сразу после загрузки, то есть практически в режиме реального времени.

Значит ли это, что Facebook знает всё о людях, с которыми вы контактируете, даже если вы не добавляли их в друзья? Вполне, если вы засветились на фото.

И как соцсеть использует эту информацию, никто предугадать не сможет. Хотя доказано, что Facebook сотрудничает с властями и предоставляет данные по запросу.

Где отключить

Функцию распознавания лиц на фото можно отключить в настройках аккаунта.

В мобильном приложении:

Зайдите в свой профиль (кнопка с тремя полосками в правом верхнем углу), нажмите «Больше» (кнопка с тремя точками под ФИО), выберите пункт «Быстрые настройки конфиденциальности». Прокрутите меню вниз, найдите пункт «Дополнительные настройки» и перейдите к пункту «Настройки распознавания лиц». На новом экране нажмите на блок «Распознавание лиц» и в появившемся меню выберите «Нет».

На компьютере:

Зайдите в настройки аккаунта (кнопка с треугольником справа на верхней синей панели, в открывшемся меню пункт «Настройки»). В левом меню выберите пункт «Распознавание лиц», нажмите на «Редактировать» или на всю строку «Распознавание лиц», затем нажмите на кнопку «Да» и в выпадающем меню выберите «Нет», после чего нажмите «Закрыть».

Выводы

Распознавание лиц в Facebook полезно или опасно? С одной стороны, это профит: Facebook сообщит, если кто-то создаст фейковый профиль с вашими фото, выложит неудачные снимки или компромат. С другой – если фото защищены настройками приватности, уведомление не придёт.

Запретить Facebook распознавать вас на фото можно в несколько кликов. После этого соцсеть сотрёт шаблон вашего лица и перестанет отправлять вам сообщения о загруженных фото с вами.

(вгору)

Додаток 6

8.03.2018

Після флешмобу «Я тобі не дорогенька» Президент більше ніколи не дозволятиме собі фамільярність, – Червак

Петро Порошенко обрав не найкращі слова, звертаючись на прес-конференції до журналіста Ірини Земляної. Тому отримав дуже гідну відповідь, у вигляді флешмобу «Я тобі не дорогенька» (ZIK).

Про це в ефірі інформаційно-аналітичного проекту «Перші про головне. Коментарі» на телеканалі ZIK говорив голова організації Українських націоналістів Богдан Червак.

«У тоталітарній країні завжди принижують жінок і вони не мають належного місця в урядуванні. Тому звернення Порошенка до журналістки Ірини Земляної на його прес-конференції «дорогенька» є нічим іншим, як висловлюванням людини, яка є вихідцем з Радянського Союзу. Таким чином він зневажливо віднісся до цієї жінки, але таке відношення він має і загалом до суспільства», – вважає народний депутат України III, VI, VII скликання Інна Богословська.

Але Богдан Червак, голова організації Українських націоналістів, вважає, що Президент України не мав на меті когось образити.

«Не хочу бути адвокатом Петра Порошенка, але мені здається, що він не ставив собі за мету образити журналісту Ірину Земляну. Просто він обрав не найкращі слова і отримав дуже гідну відповідь у вигляді флешмобу «Я тобі не дорогенька». Думаю, що після нього він більше ніколи дозволятиме собі таку фамільярність», – прокоментував Червак

За його словами, якщо він раніше вже так звертався до представниць ЗМІ, то досі просто не отримував гідної відповіді та вважає, що варто було б тепер просто перепросити.

«Я погоджуюсь з тим, що Радянський Союз та 8 березня з нас ніяк не можуть вийти, бо це станеться лише тоді, коли ми навчимося культури. Але я б ніколи такого собі не дозволив. А якби таке і сталося, то мав би сміливість перепросити, адже це є ознакою сильної людини», – наголосив він.

(вгору)

Додаток 7

28.02.2018

Все о Facebook в Украине: аудитория, реклама и рекламодатели

Компания Gemius проанализировала аудиторию Facebook в Украине, объемы размещенной там видеорекламы, а также главных рекламодателей ресурса (МедиаБизнес).

Facebook – одна из главных рекламных площадок для видео в Украине

Видеореклама в Украине ежемесячно охватывает около 80% всей интернет-аудитории в возрасте от 14 до 69 лет на ПК, и Facebook сейчас занимает вторую позицию по количеству показов рекламных роликов. На долю площадки приходится 4% всех показов видеорекламы в месяц (AdReal, ПК, январь 2018). Площадка №1 в Украине – Youtube, 47 % всех video показов отображаются на сервисе Google.

Социальную сеть Марка Цукерберга в январе 2018 года посетили 60% всей интернет-аудитории страны на персональных компьютерах и ноутбуках (11,4 млн. Real Users). За месяц пользователи сгенерировали более 600 миллионов просмотров страниц на ПК. В среднем один посетитель провел в социальной сети более 2,5 часов в месяц, тратя на визит около 8 минут (ПК). Сейчас социальная сеть занимает третью позицию по посещаемости в месяц среди ПК-аудитории и вторую – среди мобильной аудитории (смартфоны).

Facebook – в лидеры за год на ПК

Facebook с начала года укрепил свои позиции на рынке онлайн рекламы преимущественно за счет ухода рекламодателей с заблокированных российских ресурсов (Vk.com, Mail.ru, Yandex.uaи др.). В апреле социальную сеть хотя бы один раз в месяц на ПК посетили 45/ % всех пользователей Уанета, а видеореклама охватила 7 % онлайн-аудитории. Бум роста аудитории Facebook был в июне и июле 2017 года, когда более 55 % интернет-аудитории посетили социальную сеть. В июле и августе 2017 года рекламодатели сгенерировали больше всего показов и охватили аудитории на ПК (охват пользователей видеорекламой составил 20%, на 13% больше, чем в апреле).

В январе на Facebook (ПК) было сгенерировано более 28 миллионов показов видеорекламы, рекламодатели охватили в социальной сети 16% аудитории УАнета. Почти 60% видеорекламы показывались в видимой зоне экрана (viewability rate) в среднем на протяжении 8 секунд (viewability time).

Rozetka, Fotos и Allo – главные рекламодатели в Facebook

Магазины электроники стали лидерами по количеству показов видеорекламы, которые были отображены в социальной сети на ПК. Интернет-магазин Rozetka охватил в Facebook 5 % интернет-аудитории страны (3,2 миллиона показов), F.ua – 4 % (2,6 млн показов), а Allo.ua – 3,5 % (1,7 млн показов). Январь 2018.

В анализ включены данные исследований gemiusAudience (ПК-аудитория, 14-69) и gemiusAdReal (ПК-аудитория,14-69, video) за январь 2017 – январь 2018 гг.

(вгору)

Додаток 8

7.03.2018

Компании начинают активно внедрять чат-ботов

Аналитики Gartner составили прогноз по широкому распространению виртуальных клиентских помощников (virtual customer assistant, VCA) или чат-ботов в корпоративном секторе (InternetUA).

Если в 2017 году подобные сервисы использовались менее чем в 2 % операций по обслуживанию и поддержке клиентов, то к 2020 году доля возрастет до 25 %, заявил управляющий вице-президент Gartner Джин Альварес (Gene Alvarez) во время выступления на форуме Gartner Customer Experience Summit в Токио.

По его словам, больше половины компаний уже инвестировали в развитие технологий VCA для клиентского сервиса, поскольку осознают преимущества автоматизированного самообслуживания, а также способность цифровых ассистентов расширяться с функциональной точки зрения в сложных ситуациях.

«Поскольку все больше клиентов участвуют в цифровых каналах, VCA внедряются для обработки запросов клиентов на веб-сайтах, в мобильных приложениях, мессенджерах и социальных сетях, – говорит Альварес. – Это подкрепляется улучшениями в обработке естественного языка, машинным обучением и возможностями определения потребностей... Сила VCA заключается в том, что предлагать больше, чем простую информацию. Помощники должны обогащать опыт клиентов, помогать им взаимодействовать с компанией и обрабатывать транзакции от имени клиентов».

По данным исследования Gartner, после внедрения виртуальных клиентских помощников количество обращений через телефон или электронную почту снижается на величине до 70 %. При этом растет удовлетворенность заказчиков и экономится около 33 % времени на разговоры с ними.

84 % опрошенных организаций заявили о планах по увеличению в 2018 году расходов на технологии, направленные на повышение качества обслуживания клиентов.

В докладе Gartner также прогнозируется, что к 2019 году около 20 % брендов откажутся от использования фирменных мобильных приложений, поскольку они не обеспечивают ожидаемый компаниями уровень привлечения и удержания клиентов.

Первоначальные расчеты по окупаемости инвестиций в создание ПО для смартфонов и планшетов оказались неверными из-за расходов на поддержку, обновления, маркетинговое продвижение и др. Теперь бренды вкладывают деньги в развитие канала общения в популярных мессенджерах, вроде Facebook Messenger и WeChat.

(вгору)

Додаток 9

13.03.2018
Соцмережі: вільний обмін думками чи згубна звичка
Громика Наталія

Про невидимі загрози віртуального світу, інтернет-ширму, за якою мільйони користувачів приховують своє справжнє «я», лайки як гормон росту самооцінки і про те, як не стати заручником образу, створеного онлайн та чому корисно мати власні сторінки у соцмережах розповіла психолог-психотерапевт, кандидат психологічних наук, доцент кафедри практичної психології Сумського державного педагогічного університету ім. А. С. Макаренка Дар'я Черенщикова (Трибуна).

Якщо ти не «лайкав», не «репостив», поснідав і не поділився фоткою смакоти на тарілці з інтернет-спільнотою – день пройшов дарма. За такими правилами нині живе більшість з нас. Іноді ми навіть не підозрюємо, що підсвідомо вже давно стали рабами соцмереж, а життя стрімко перетворюється на самопіар онлайн чи такий собі батл «хто крутіший».

«Для мене як для фахівця соцмережі постають джерелом надзвичайної невротизації. В силу, можливо, пошкодженої самооцінки або тривожності, притаманній людині, в силу якихось внутрішньо-особистісних переживань, ми можемо спостерігати за життям інших людей і завжди на їхньому фоні відчувати себе недостатньо гарним, добрим, розвиненим, активним, енергійним або безліч інших варіантів. Тобто коли я спостерігаю за тим, як інші люди кудись подорожують, відвідують якісь події, заходи, щось продукують, виробляють, чимось займаються і я на їхньому фоні "не такий", то моя невротизація буде посилюватися, а самооцінка, начебто "вдарятися"», – констатує Дар'я Черенщикова

Веб-театр: що приховують за онлайн-маскою завсідники соцмереж

Інтернет відчинив двері у квартири друзів та ворогів. Лише кілька кліків і ми знаємо, де та з ким відпочивав колишній, що на обід у подруги, як провів вікенд колега, якого кольору шпалери у будинку однокласниці, котра днями повернулася із заробітків і т. д.

«Соціальні мережі – це психологічно безпечний простір, тобто я можу на себе приміряти будь-який образ, маску, роль, таким чином представляю загалу "уявлюване я", ідеальний образ себе. Для мене це безпечне, адже ніхто ніколи не здогадається про це, ніхто мене реального не побачить, тому відсутність самого контакту, в якому можуть проявитися будь-які мої сторони, дає можливість проявлятися моїм бажаним рисам. Це називається або "персона", або "роль", або "маска". Такий образ, який ми проявляємо через інтернет, він отримує більше заохочення, психоемоційних погладжувань у вигляді лайків. Від природи кожен із нас прагне заохочення. Якщо я знаю, що в цьому образі я це погладжування отримую, то цей образ буде для мене більш привабливим, тому мені в ньому значно комфортніше, ніж в реальній реальності».

Життя online затягує. Замість сніданку, обіду й вечері – чергова порція фото у стрічці новин. Інтернет-океан вирує. Наталя разом зі своїм коханим рвонула у тур Європою. Максим, якого вважала безперспективним «нарцисом», одружився. Євгенія, котра з «золотом» покинула стіни рідної школи, нині надія вітчизняної науки, знову якийсь грант отримала. А Оксана, будні якої

вписуються у трикутник «дім-робота-дім», спостерігає за цим і вважає себе сірою мишкою.

«Людина, у якої з самооцінкою з самого початку все добре, вона звісно щиро буде радіти за інтернет-друзів, котрі активно себе проявляють, а успіхи інших стануть для неї позитивною мотивацією до підкорення нових вершин. Там, де є ознаки невпевненості заниженої самооцінки, слабкої самоцінності, то такі пости інших людей викликатимуть почуття тривоги (“ я не встигаю”, “а в мене не так”, “я гірший”), тоді спрацьовує мотивація на уникнення невдачі».

Психолог Дар’я Черенщикова каже, що часто-густо солодке життя інтернет-друзів не що інше, як картинка на заздрість усім. Здебільшого за лаштунками лакшері-аккаунтів – буденні персонажі.

«Ми забуваємо інколи, що те, що висвітлюють наші друзі у соцмережах, воно, по-перше, не завжди відповідає дійсності, по-друге, слід пам’ятати про те, що якби ми виставляли події свого життя так само, то наше життя проявилося по-іншому, ми би самі побачили його значно яскравішим, аніж уявляємо».

Інтернет: симптоми залежності та правильне дозування

Тих, хто «підсів» на систематичні подорожі віртуальним світом, розпізнати не важко. Вони забувають про сон та їжу. Соцмережі буквально виривають їх зі звичної реальності, а відокремити себе інтернетного від себе як особистості їм вже не під силу.

«Ознакою інтернет-залежності є той факт, коли там (у віртуальному світі) мені краще, ніж зовні (у реальності), а в проведення часу за комп’ютером я вкладаю набагато більше власного ресурсу, ніж я можу. Наприклад, раніше, коли інтернет не був безлімітний це було дуже яскраво видно на грошах, коли ми вкладали надзвичайно великі суми коштів у інтернет. Зараз, коли доступ до глобальної павутини здебільшого необмежений, про інтернет-залежність свідчить кількість часу, проведеного онлайн.

Тривожним сигналом слід вважати і надто сильний механізм втечі, коли людина не може контактувати ані з собою, ані з реальним світом та шукає будь-які способи, аби поринути у веб-простір та відчуває в цьому постійну потребу на фізіологічному рівні.

Час витрачений на інтернет не повинен заважати роботі та живому спілкуванню, а також не конфліктувати з базовими, фізіологічними потребами людини, такими як: сон, їжа і навіть туалет. До того ж, соцмережі не мають суперечити соціальним ідентичностям, тобто користувач може повноцінно виконувати функції “батько”, “мати”, “брат”, “сестра”, професійні ідентичності “студент”, “начальник” або “школяр», – говорить Дар’я Черенщикова.

Соцмережі як майданчик комунікації

Абсолютного зла не буває. Сцмережі можуть бути надійними і прогресивними помічниками. Для людей, котрі використовують соцмережі переважно для спілкування, при цьому не зависають в інтернеті цілодобово, це своєрідний тренажер для комунікативних навичок. Ті, хто здатні з розумом розпорядитися новітніми інструментами, в «реалі» швидше знаходять спільну мову з незнайомцями, без проблем адаптуються в новому колективі.

«Соціальні мережі несуть надзвичайно велику користь. По-перше, це можливість спілкування, коли відсутні інші умови для комунікації. По-друге, це можливість обмінюватися досвідом, новинами, запрошувати на події, за когось навіть порадіти ,знаєте хтось виставляє якісь пости, а ми можемо радіти. Ми можемо спостерігати за життям іншої людини, чим вона займається, навіть якщо у повсякденному житті я з нею не спілкуюся, я слідкую за контекстом її життя і таким чином з нею в контакті. Це змушує мене так само розвиватися, проявляти якусь активність і т. д. Дехто навіть використовує соціальні мережі у комерційних цілях, може робити рекламу власних продуктів, проектів, послуг і це достатньо доступно і цікаво. А ще у соціальних мережах ми можемо просто відпочивати», – певна Дар'я Черенщикова.

Відтак, фахівці рекомендують, аби не потрапити в тенета глобальної павутини і по максимуму раціонально використовувати соцмережі слід контролювати час прогулянки веб-просторами, «ходити» в інтернет з конкретною метою, для виконання необхідних завдань, а ще не забувати про живе спілкування,яке не можуть замінити жодні суперсучасні гаджети.

Дар'я Черенщикова наголошує: «Варто пам'ятати те, що соціальні мережі – це не спосіб життя, а лише засіб, який допомагає спілкуватися, контактувати, обмінюватися інформацією. Реальна реальність завжди сильніша за будь-яку віртуальну. За чим би ви не спостерігали в соціальних мережах ваше реальне життя наповнене, насичене, воно іде і відбувається. Найцінніше у цьому світі – безпосередньо ви і ваше життя у ньому, все інше – деталі. Щастя не потребує висвітлення, його варто розділяти і проживати з найближчими людьми».

(вгору)

Додаток 10

13.03.2018

Ученые нашли в смартфонах неожиданную опасность для здоровья

Эндокринолог Роберт Люстиг рассказал все подробности проведенного исследования (Сегодня).

Ученые выяснили, что смартфон может вызвать проблемы с психикой у своего владельца. Постоянные звонки и оповещения подталкивают гормоны стресса к действию, постоянно вызывая защитную реакцию «бей или беги». Это привело к тому, что 89 процентов американских студентов жалуются на «фантомные» виброзвонки – когда мозг реагирует на телефон, даже если тот отключен. Еще 86 процентов американцев утверждают, что постоянно проверяют электронную почту и соцсети, пишет Business Insider.

Эндокринолог Роберт Люстиг рассказал порталу, что телефонные уведомления «тренируют» мозг находиться в почти постоянном состоянии стресса и страха. Это приводит к тому, что префронтальная кора головного мозга, отвечающая за когнитивные функции высшего порядка (саморефлексия, воля, абстрактное мышление, самовосприятие и метазнание), перестает функционировать в полном объеме.

«Вы заканчиваете глупыми вещами, которые могут привести к беде», – утверждает Люстиг.

По утверждению ученых, 97,5 процента людей не способны к настоящей многозадачности. Если человек чем-либо занят, ему приходится прерываться, чтобы ответить на телефонный звонок, и в случае замешательства повышается уровень гормона стресса кортизола, для нейтрализации которого мозгу требуется гормон радости дофамин. Другими словами, накапливаемый стресс при попытке сделать много вещей сразу приводит к болезненным состояниям.

(вгору)

Додаток 11

13.03.2018

Британский hr-менеджер рассказала, как должен выглядеть ваш профиль в соцсетях

При поиске новой работы не забудьте заглянуть в свои профили в социальных сетях. Британский hr-менеджер рассказала изданию Daily Mail о том, почему профиль кандидата может стать решающим фактором при приеме на работу и как заставить соцсети работать на вас, а не против вас (Телекритика).

Использование социальных сетей в последнее десятилетие развилось до невероятных масштабов. Некоторые из нас не выпускают смартфон из рук 24 часа в сутки. Границы личного пространства и конфиденциальности слишком размыты в современном мире.

Сотрудники крупных компаний предпочитают Facebook, Instagram, Twitter и профессиональную соцсеть LinkedIn. Однако важно помнить, что комментарии, фотографии и подписи, которыми вы делитесь в интернете, являются вашим лицом.

Пэм Линдсей-Данн, региональный hr-директор Hays & James Innes, которая написала ряд книг по всем аспектам поиска работы, дает советы соискателям.

1. *Сделайте профили приватными*

Согласно недавнему опросу, 7 из 10 потенциальных работодателей используют социальные медиа для изучения кандидатов перед интервью и непосредственным наймом. Несмотря на это, только треть кандидатов уверены, что этот этап проверки вообще состоится.

Пэм Линдсей-Данн считает, что перевод учетных записей в «приватные» – лучшее, что вы можете сделать.

2. *Сохраняйте позитивный настрой*

Как отмечает специалист, социальные медиа следует вести в позитивном ключе, особенно профиль в LinkedIn.

«LinkedIn – отличный способ продемонстрировать страсть к вашей отрасли, вступив в соответствующие группы, регулярно публикуя информацию

и обновляя свой профиль, – говорит Пэм. – Если ведете LinkedIn, убедитесь, что ваше резюме соответствует вашему профилю по срокам и опыту работы».

3. *Следите за активностью в соцсетях*

Фото, пост, снова фото, снова пост – и все это в рабочее время. Так не годится, уверена эксперт. Внезапное увеличение активности в социальных сетях в рабочие часы является признаком того, что вы тратите много времени на посторонние занятия, а значит, ваша производительность на работе невысока.

4. *«Зачищайте» ненужный контент*

Задумайтесь, что ваш профиль в социальных сетях говорит о вас? Все, что вы когда-либо делали в интернете, будет доступно работодателю.

(вгору)

Додаток 12

2.03.2018

Голова Держкомтелерадіо Олег Наливайко взяв участь у дискусії щодо протидії фейкам

Голова Держкомтелерадіо Олег Наливайко взяв участь у слуханнях «Стопфейк: проблема законодавчого регулювання відповідальності за дифамацію у медіа», які відбулися в Комітеті з питань свободи слова та інформаційної політики Верховної Ради України (Державний комітет телебачення і радіомовлення України).

Учасники дискусії – представники органів державної влади, журналісти, медіа експерти, юристи – обговорили міжнародний досвід боротьби з фейками та шляхи протистояння України гібридній війні.

Як зазначали промовці, країни Заходу шукають відповіді на виклики сучасності. Наприкінці 2017 року Єврокомісія оголосила про початок публічних дебатів на тему, як протидіяти фейкам у новому інформаційному суспільстві. У січні цього року почала працювати комісія незалежних експертів, яка має на меті розробку документів для Європейського Союзу. Це дасть інструменти для визначення, що таке «фейкові новини», а також для боротьби з цим явищем. Крім того, у Німеччині прийнято закон про боротьбу з дифамацією в соцмережах. У Великобританії та Італії теж триває збір пропозицій про те, як протистояти фейковим новинам. У Франції готується законопроект, за яким національний регулятор у випадку прийняття зможе позбавляти мовників ліцензії, якщо буде доведено іноземний вплив при втручанні у вибори.

Про актуальність цієї проблеми для України, про необхідність посилення боротьби з фейками в інформаційній сфері говорили учасники парламентських слухань. Вони наголосили, що при підготовці змін до законодавства слід взяти за основу відповідні документи Ради Європи, які диференціюють неправдиву інформацію, поділяючи її на ту, яка є наслідком поганої, себто непрофесійної

журналістики, джинсу (замовні матеріали), маніпуляції та дезінформацію, щодо якої є чіткі критерії.

Голова Комітету з питань свободи слова та інформаційної політики Вікторія Сюмар наголосила, що всі пропозиції, які були озвучені на слуханнях, будуть проаналізовані та знайдуть своє відображення у відповідних рекомендаціях.

(вгору)

Додаток 13

28.02.2018

Майя Яровая

Нацполиция предлагает блокировать сайты, ссылаясь на европейские нормы. Что с этим не так

На украинском рынке телекоммуникаций обсуждают очередной законопроект, в котором под видом европейских норм продвигают совсем не европейские практики – в частности блокировку сайтов. Изначальная редакция закона вызвала много замечаний, однако несмотря на усилия участников рынка, в новой редакции они не были учтены (AIN.UA).

Проект предложила Национальная полиция еще весной 2017 года, его цель – имплементация в украинское уголовное законодательство норм Конвенции о киберпреступности, одобренную Советом Европы в Будапеште в 2011 году. Преимущественно речь в законе идет о порядке следственных действий при раскрытии киберпреступлений. Однако между делом в него вписали положения о блокировке сайтов, которые к конвенции не имеют отношения и не упоминают в ней.

Положения, которые вызвали негативную реакцию участников рынка, выделил председатель ИнАУ Александр Федиенко. Помимо блокировок сайтов, в законопроекте также содержатся требования к провайдерам предоставлять по запросу спецслужб и правоохранительных органов персональные данные об «особах конечных пользователей» (причем, термин «конечный пользователь» в проекте не определен) и хранить их данные и трафик не менее 90 дней. По мнению экспертов, такие требования не соответствуют Европейскому праву.

«ИнАУ ранее направляла по предварительным версиям этого ЗП ряд замечаний. Кое-что из второстепенных замечаний учтено, но ключевые моменты в этом последнем варианте не учтены. Самое главное: под названием имплементации Конвенции туда подсовывают блокирование доступа к сайтам. В Конвенции по киберпреступности (Будапештская конвенция) о блокировании доступа – ни слова», – сообщил AIN.UA исполнительный директор ИнАУ Владимир Куковский.

«Насколько я сейчас понимаю, их «хитрость» – в «неправильном» переводе понятия Freezing доступа – одного из ключевых понятий Конвенции, – пояснил директор NetAssist Максим Тульев в комментарии AIN.UA. – Идея

Freezing – в том, что следователь, видя на его взгляд нарушение закона ресурсом интернета, немедленно выдаёт оператору или хостеру ордер на заморозку данных. Это НЕ блокировка ресурса – ресурс остается доступным в штатном режиме. Это ордер, который запрещает клиенту и хостеру что-либо изменять в контенте, логах, данных – чтобы специально или случайно не уничтожились улики преступления. Иногда дается еще и ордер оператору сохранять весь проходяший к этому ресурсу трафик».

Далее следователь идет к судье и получает судебный допуск к данным, получает сами данные (доказательства) в неизменном виде. Или не получает, если судья решит, что основания недостаточны. «Как по мне, очень правильная тема. Вот только этот фризинг к блокировке доступа не имеет ни малейшего отношения», – заключил Тульев.

Целиком проект закона опубликовал у Максима в Facebook. «Как обычно, россиян не только догоняем, но и сразу перегоняем на голову», – написал он.

Закон еще не подан в парламент. Сейчас проходит процедура согласования проекта с госорганами, в рамках которой его вчера одобрила НКРСИ, но с рядом существенных замечаний. Регулятор предлагает «доработать проект Закона с целью приведения его в соответствие с Конвенцией про киберпреступность». В частности, указать, что блокировке должен подвергаться не весь сайт, а только запрещенная информация.

«Закон об имплементации Конвенции должен быть посвящен исключительно имплементации Конвенции. А по блокированию сайтов пусть предлагают и продвигают другой закон, и убеждают парламент», – подчеркнул Куковский.

Проект сравнивают со злополучным №6688, который в итоге провалился на голосовании. Напомним, в проекте закона, в частности, предлагали разрешить блокировать доступа к ресурсам по ходатайству следователя или прокурора следственным судьей. Но в особо «неотложных случаях, связанных со спасением жизни людей или предотвращением особенно тяжкого преступления» – без решения суда на 48 часов.

(вгору)

Додаток 14

6.03.2018

Еврокомиссия потребовала удалять террористический контент из соцсетей в течение часа

Европейская комиссия опубликовала новые правила для социальных сетей, согласно которым они должны удалять террористический контент не более чем через час после того, как о нём станет известно. Ранее орган исполнительной власти потребовал у Facebook, Twitter, YouTube и Microsoft более эффективно бороться с ненавистной речью, и это требование подействовало. Теперь Еврокомиссия хочет, чтобы так же произошло и с публикациями и файлами, пропагандирующими терроризм (InternetUA).

«Онлайн-платформы становятся главным способом получения информации, поэтому они несут ответственность за создание безопасного окружения для своих пользователей, – заявил вице-президент Еврокомиссии Андрус Ансип (Andrus Ansip). – То, что незаконно за пределами Сети, незаконно и в ней. Некоторые платформы стали удалять больше нелегального контента, чем когда-либо прежде – и это показывает, что саморегулирование работает, – но нам всё ещё нужно начать быстрее реагировать на террористическую пропаганду и другой нелегальный контент, который является серьёзной угрозой безопасности, сохранности и основным правам наших граждан».

Еврокомиссия потребовала проверки и удаления террористического контента в течение часа после того, как о нём кто-то сообщит, поскольку «в первые часы присутствия в Сети он несёт наибольший вред». Орган власти также попросил социальные сети улучшить системы автоматического обнаружения опасного содержимого, чтобы они могли не так сильно полагаться на сообщения людей. Наконец, Комиссия потребовала делиться системами обнаружения с другими компаниями и более тесно работать с правоохранительными органами.

(вгору)

Додаток 15

28.02.2018

Волинянин розповсюджував мобільний додаток, який «краде» гроші з рахунків

Історія про те, як двоє вмілих та перспективних студента вирішили нелегально підзаробити. Маючи навички програмування, вони розробили власний мобільний додаток, за допомогою якого отримували доступ до банківських рахунків користувачів мобільного банкінгу (InternetUA).

Один із них – 24-річний волинянин – використовуючи мову програмування Java та інструменти SDK (від англ. softwareDevelopmentKit) протягом кількох років вивчав, розробляв та тестував власний TrojanBot-додаток для прихованого віддаленого управління користувацькими даними, які зберігаються на мобільному пристрої Android.

Шкідливе програмне забезпечення, мало кілька версій для маскування під легальні Android-програми та поширення користувачам мережею Інтернет. Наприклад, під додаток для пошуку друзів у соціальних мережах або під додаток для знайомств та побачень.

Після встановлення на мобільний пристрій TrojanBot перевіряв наявність адмінправ (root) програм «мобільного банкінгу», отримував детальну інформацію щодо номера телефону, IMEI, геолокації та інших ідентифікаторів жертви, налаштовував перехоплення та приховану відправку смс-повідомлень.

У шкідливому коді зловмисники розмістили скрипт, який здійснював моніторинг балансу та транзакцій всіх без виключення фінансових додатків

пристрою, збір логінів та паролів. Результати роботи TrojanBot відправлялися на управляючий сервер зловмисників погодинно.

Аби шкідливе програмне забезпечення не було ідентифіковане антивірусами для Android, його спільник модифіковував готові APK файли із Trojan-Bot, щоб приховати сигнатури коду прихованого віддаленого управління користувацькими даними. Також, він винаймав та налаштовував приватні віртуальні сервери для розміщення ряду адміністративних Bot-панелей.

Зловминики поширювали додатки для пошуку друзів у соціальних мережах та додатки для знайомств і побачень за допомогою веб-форумів користувачів Android. Таким чином, вони інфікувати більше шести тисяч пристроїв громадян України, США, країн Євросоюзу та Азії.

Під час розслідування, працівники кіберполіції встановили усі переписки зловмисників та обмін вихідними кодами шкідливого програмного забезпечення, адреси розміщення серверів адміністративних Bot-панелей. Крім того, встановлено і Інтернет-сторінки з готовими APK файлами Trojan-Bot, властивості та вміст Bot-панелей і Trojan-Bot, дані жертв зловмисників.

Більше того, для приховання слідів своєї злочинної діяльності, під час обшуку один із зловмисників намагався пошкодити свою комп'ютерну техніку.

На даний час слідство триває у межах розпочатого кримінального провадження за ч. 2 ст. 361-1 КК України. 24-річному волинянину та 19-річному уродженцю Херсонщини загрожує до п'яти років ув'язнення.

(вгору)

Додаток 16

1.03.2018

Пользователям советуют срочно удалить популярное приложение

Изначально приложение GetContact разрабатывали как блокировщик SMS-рассылок и нежелательных звонков. А потом разработчики решили пересмотреть функциональность программы и добавили любопытную фичу.

GetContact позволяет узнать, как ваши близкие и друзья записали вас в свою телефонную книгу. Просто вводите номер телефона человека, на смартфоне которого вы хотите увидеть свое записанное имя (InternetUA).

Идея действительно интересная, но на самом деле все не так просто. Если копнуть немного глубже, вы поймете, что GetContact банально ворует конфиденциальную информацию и парсит телефонную книгу с вашего смартфона.

Избегайте GetContact и его аналогов

Вряд ли вам будет приятно, если кто-то будет копаться в ваших личных вещах, а потом сравнивать их с другими.

А вот GetContact делает именно так. Анонимно собирает базу контактов и пересылает на удаленный сервер. Чем в этот момент занимаются цензоры Apple – неизвестно.

К слову, приложение успели заблокировать в Казахстане и на территории Азербайджана, но в App Store тут же появился аналог – GetContact_. Да, вот так с помощью нижнего пробела разработчики обошли запрет.

А что делать, если я уже в базе?

Разработчики сервиса предусмотрели возможность удаления из базы, при условии, что вы уже устанавливали приложение ранее.

Шаг 1. Открываете GetContact на смартфоне и удаляете аккаунт (Настройки учетной записи —> Удалить аккаунт).

Шаг 2. Открываете официальный сайт сервиса и во вкладке Unlist указываете свой номер.

В течение суток с момента подачи заявки на удаление, ваш номер пропадет из базы GetContact.

P.S. на будущее. Старайтесь избегать приложений, которые предлагают подобные функции. Пару минут хорошего настроения могут стоить сливу всей базы контактов. Вряд ли вам это нужно.

(вгору)

Додаток 17

5.03.2018

Що про вас знає Facebook, навіть якщо його у вас немає. 38 фактів

Facebook може відслідковувати ваші рухи онлайн, навіть якщо ви ніколи не відвідували сайт цієї соціальної мережі (InternetUA).

Про те, що найбільша соціальна мережа у світі створює секретні файли про діяльність мільярдів людей, пише The Daily Mail.

Компанія Марка Цукенберга запевняє, що використовує цю інформацію для цільвої реклами та формування контенту, який будується на наших вподобаннях, а також задля забезпечення безпеки.

Власники аккаунтів у Facebook можуть завантажити копію файлу, у якому зібрана вся інформація про них, але конфіденційність користувачів, які відстежується третіми особами, наразі під питанням.

Це означає, що існує тільки один шлях побачити, якою інформацією володіє Facebook, – створити власний аккаунт.

Так, отримати доступ до файлу з вашими даними у Facebook можна зайшовши у «Налаштування» і далі натиснувши «Завантажити копію ваших даних з Facebook».

Отримати доступ до файлу з вашими даними у Facebook можна зайшовши у «Налаштування».

Репортер New Zealand Herald Нік Вігам вирішив протестувати, що Facebook знає про нього, та був здивований результатом.

У 2010 році компанія Facebook стала першою соціальною мережею, яка надала користувачам можливість завантажувати файли, що містять свою особисту історію, на сервісі.

Серед інформації, зібраної компанією на репортера, був мобільний запис старого відео з його мамою, яка обіймала Вігама у перший його день у школі.

Він також наткнувся на відсканові копії договорів оренди, рахунки за його домашні послуги, знімки банківських переказів, а також більш банальні журнали чатів та іншу історію сайту.

Для своєї роботи Facebook використовує дані, зібрані від 1,4 мільярда активних користувачів з усього світу, в якості основи для алгоритмів, які пов'язують рекламу та інші матеріали з онлайн-профілем людини.

Зокрема, ця соціальна мережа може збирати дані про всю діяльність в інтернеті, починаючи від пошуку та історії чату в Messenger і закінчуючи завантаженими фотографіями та файлами, що надсилаються на його сервери.

Крім того, Facebook використовує плагіни та файли-cookie – інструменти, які відстежують діяльність користувача в інтернеті, – для збору даних через сторонні веб-сайти.

Щоразу, коли ви ставите лайк, поширюєте контент у Facebook або відвідуєте сайти через додатки цієї соціальної мережі, за вами стежать.

Навіть якщо ви ніколи не заходили на сайт Facebook, компанія все ще може відстежувати вашу діяльність у брайзері без вашого відома.

Більш ніж 10 тисяч веб-сайтів складаються з невидимих трекерів, які називаються пікселями. Вони записують інформацію про те, якою операційною системою ви користуєтеся, яка ваша IP-адреса, яку активність на веб-сайті ви здійснюєте продовж відвідування.

Це дозволяє компанії знати все, починаючи з того, де ви знаходитеся, хто є вашим інтернет-провайдером, які типи сайтів вам подобаються та скільки часу ви витрачаєте на їх відвідування.

Занепокоєння щодо відстеження активності соціальною мережею та обробкою конфіденційної інформації вже притягнули компанію Facebook до юридичної відповідальності.

У лютому 2018 року бельгійський суд постановив зупинити відстеження діяльності бельгійських користувачів інтернету, які не мають аккаунту у соцмережі або штрафуватиме компанію на 250 000 євро на день.

Напротивагу Facebook вважає, що файли-cookie та пікселі використовуються відповідно до технологічних стандартів.

«Ми побудували команду людей, які фокусуються на захисті конфіденційності, від інженерів до дизайнерів, й інструменти ці дозволяють людям обирати і контролювати», – заявив Facebook.

(вгору)

Додаток 18

5.03.2018

1+1 медіа запускає комерційний проект для захисту авторських прав в інтернеті

Група «1+1 медіа» оголосила про запуск нового комерційного продукту SUDUM – технологічно-правової системи для захисту авторських прав в інтернеті, яка допомагає блокувати нелегальні копії відеоконтенту на сайтах, популярних соціальних мережах та відеохостингах (МедиаБизнес).

SUDUM в автоматичному режимі 24/7 проводить пошук нелегальних копій відео в інтернеті. Після виявлення піратських версій контенту, програма самостійно розсилає скаргу веб-сайту, хостинг-провайдеру або адміністрації соціальної мережі, в залежності від майданчика, де був розміщений контент. Роботу системи контролюють фахівці 1+1 медіа для того, щоб уникнути випадкового блокування легального контенту.

SUDUM був розроблений департаментом 1+1 Digital для захисту власного контенту медіахолдингу від піратів. Після першого року роботи системи, 1+1 медіа вдалося досягти 94 % ефективності зачистки нелегального відео в інтернеті: було видалено 200 тис. копій, а прибуток, від збільшеного трафіку на онлайн-ресурсах групи, виріс на 40 %.

«Інтернет-піратство – суттєва проблема для правовласників, та одна із головних причин, із-за якої вони недоотримують прибуток. Сьогодні виробники контенту об'єднуються для вирішення цієї проблеми. Для нас важливо бути компанією, що не тільки бореться з піратами, а й пропонує ринку свої рішення для боротьби з ними. Ми маємо багатий досвід захисту власного контенту і готові його масштабувати на бізнеси інших правовласників», – відзначає Анна Ткаченко, директор діджитал-напрямку 1+1 медіа.

Сьогодні SUDUM здатний забезпечити захист інтересів правовласників в рунеті та уанеті, а першими клієнтами 1+1 медіа стали KINOMANIA, KINOLIFE Distribution, Must See Movie та Ukrainian Film Distribution.

В плани з розвитку SUDUM входить розширення типів контенту, які може захищати система: аудіофайли, тексти, графічні зображення. Крім того, в разі успіху на українському ринку, 1+1 медіа планує запропонувати своє рішення закордонним правовласникам.

(вгору)

Додаток 19

6.03.2018

Россия использует Украину, как тестовую площадку для кибератак – МВД Великобритании

Главы МВД Украины и Великобритании Арсен Аваков и Бен Уоллс на встрече обсудили планы по совместной отработке механизма борьбы с киберпреступностью и организованной преступностью между странами. О встрече министров, которая прошла в Лондоне, сообщает Департамент коммуникации МВД Украины (InternetUA).

Свою обеспокоенность кибератаками на Украину со стороны России выразил британский министр.

«Правительство Великобритании обеспокоено, что Украину используют как тестовую площадку для кибератак, для развития организованной преступной деятельности и коррупции со стороны Российской Федерации», – отметил Уоллс.

Британский министр также добавил, что МВД Великобритании заинтересовано в углублении сотрудничества с коллегами из Украины.

«Мы заинтересованы углубить с вами сотрудничество как в правоохранительной сфере, так и в координации действий по нелегальной миграции и оперативному обмену данными. Понимаем, какое давление на вас оказывает ваш сосед, и как вам не просто работать в этих условиях», – рассказал Уоллс.

В свою очередь, Аваков отметил, что за последние три года Украина получила успешный опыт реализации международных операций.

«За последние три года мы вывели на высокий уровень работу наших киберподразделений. Мы имеем успешные реализации международных операций. В частности, недавно в Киеве полицейские задержали организатора международной преступной платформы, известной как Avalanche, которая ежедневно инфицировала по всему миру до полумиллиона компьютеров», – рассказал украинский министр.

Он также добавил, что МВД Украины и Национальная полиция готовы усилить сотрудничество с полицией Великобритании по всем направлениям криминального блока.

«Мы готовы сотрудничать в сфере борьбы с организованной преступностью и предоставлять оперативную информацию в двустороннем порядке, чтобы этот механизм работал, как часы», – отметил министр внутренних дел Украины.

(вгору)

Додаток 20

12.03.2018
Роман Черный
Киберпреступники натравят на вас искусственный интеллект

Представьте себе следующую ситуацию. Вы получаете звонок или голосовое сообщение от близкого человека, который сейчас путешествует за границей. Он утверждает, что потерял телефон и деньги и просит вас о помощи. Ранее вы получали электронные письма с подобными просьбами, но, будучи технически подкованным человеком, решили, что вас пытаются «развести». Но на этот раз никаких сомнений нет – вы собственными ушами слышите голос своего знакомого. Вы переводите деньги. И напрасно. Ведь этот голос сгенерирован при помощи искусственного интеллекта. Из соцсетей преступники получили все необходимые сведения, включая образцы голоса потенциальной жертвы. Затем – сформировали соответствующие голосовые сэмплы при помощи интеллектуального алгоритма (IGate).

Пока это – вымышленный сценарий. Но последние успехи искусственного интеллекта делают такое развитие событий все более вероятным. К примеру, самообучающейся системе Google DeepMind AlphaZero понадобилось всего восемь часов, чтобы научиться играть в древнюю китайскую игру Go лучше, чем любому из людей. Подобные самообучающиеся алгоритмы могут быть крайне полезны в науке и экономике.

Палка о двух концах

Как показывает отчет «Злонамеренное использование искусственного интеллекта», опубликованный недавно исследовательской компанией OpenAI, эта технология может стать палкой о двух концах. С одной стороны, ИИ будет и дальше делать жизнь людей лучше. С другой, преступники, террористы и страны-изгои будут эксплуатировать этот мощный инструмент, чтобы вредить другим.

Злонамеренное использование искусственного интеллекта угрожает не только собственности и приватности людей. В более тревожных сценариях оно может угрожает их жизням. В мире быстро увеличивается количество дронов и других киберфизических систем, вроде беспилотных автомобилей или умных медицинских устройств. Все они могут становиться заманчивыми целям для террористов и киберпреступников. Возможные сценарии включают множество пугающих вещей – от спровоцированных автокатастроф до дронов, узнающих жертву в лицо.

Мир постправды

Еще один пугающий способ применения искусственного интеллекта - влияние на умы людей. Недавно спецпрокурор Соединенных Штатов Роберт Мюллер, возглавляющий расследование ФБР о вмешательстве России в президентские выборы США, заявил, что над процессом срыва голосования в 2016 году работала профессиональная команда из восьмидесяти человек.

А теперь представьте, что в руки такой команды попадает алгоритм, позволяющий создавать поддельные видео, неотличимые от реальных, или поддельные аудиодорожки с голосами любой публичной персоны.

Инструменты, которые позволяют менять лица людей на видео, уже существуют. Пользователь Reddit под логином Deepfakes первым начал использовать подобный алгоритм, чтобы «приклеивать» лица голливудских звезд к телам порноактрис. Пока технология несовершенна, но рано или поздно поддельные видео станут соврешенно неотличимыми от реальных. видеороликов. Проще говоря, любой человек сможет создать реалистичный видеоролик с участием любого другого человека.

Эксперты OpenAI опасаются, что это приведет к окончательной потере какой бы то ни было истины. Представьте, что вам удалось запечатлеть чиновника, берущего крупную взятку. Такое видео больше не будет являться доказательством для обвинения в коррупции. Чиновник просто скажет, что это видео поддельное. И в доказательство представит сотню не менее реалистичных видеороликов, где взятку берут самые разные персоны разной степени абсурдности, от Люка Скайуокера до Папы Римского.

Справедливо и обратное. Умные алгоритмы неизбежно будут использоваться для создания компрометирующих материалов на вполне честных людей. И хотя в подобном «мире постправды» видео перестанет являться объективным доказательством чего-либо, поддельные ролики все же смогут подмочить чью-то репутацию и посеять в массах сомнения.

Забудьте о блестящих журналистских расследованиях и разоблачениях, меняющих ход истории. Искусственный интеллект способен окончатлельно уничтожить песчинки правды, похоронив их в океане фейков. А значит, миром будут править наиболее отъявленные лжецы и подонки.

(вгору)

Додаток 21

12.03.2018

Уязвимости в Facebook раскрывали списки друзей и платежные данные

Исследователь безопасности Йосип Франькович (Josip Franjković) обнаружил в приложении Facebook для Android уязвимости, позволяющие получить доступ к списку друзей пользователей соцсети и узнать их платежные данные (InternetUA).

У Facebook есть конечная точка GraphQL, использующаяся только некоторыми приложениями от самих разработчиков Facebook, пояснил Франькович. Как правило, для запроса GraphQL необходим токен доступа (access_token) пользователя или страницы.

«Я решил попытаться использовать клиентский токен приложения Facebook для Android, но конечная точка вернула сообщение об ошибке. Я не отправлял постоянный запрос, однако в сообщении сообщалось, что разрешены только постоянные запросы из белого списка. Поскольку я собираю постоянные GraphQL-запросы Facebook, я решил запустить парочку из них и посмотреть, есть ли они в белом списке», – сообщил Франькович.

Исследователю не удалось найти запрос из белого списка – каждый раз появлялось одно и то же сообщение об ошибке. Тогда он вспомнил о другом способе отправки постоянных запросов, предполагающем использование doc_id в качестве ID запроса. Сообщение об ошибке больше не появлялось, но практически каждый раз ответ содержал публично доступные данные. Тем не менее, на запрос «CSPlaygroundGraphQLFriendsQuery» исследователь получил ответ со списком друзей, несмотря на установленные пользователем настройки конфиденциальности.

Франькович уведомил Facebook о проблеме в начале октября прошлого года, и компания вскоре исправила ее.

Как уже упоминалось, исследователь также обнаружил уязвимость, раскрывавшую платежные данные любого пользователя Facebook. Проблема в Graph API позволяла с помощью поля payment_modules_options получить такие данные, как первые шесть цифр номера банковской карты, указывающие на

банк-эмитент, последние четыре цифры, месяц и год истечения срока действия карты, тип карты, имя держателя карты, индекс и страну.

Франькович обнаружил уязвимость, перехватив все запросы, отправляемые приложением Facebook для Android в процессе регистрации и авторизации. Исследователь сообщил о ней Facebook 23 февраля текущего года, и спустя 13 часов проблема была исправлена.

(вгору)

Додаток 22

13.03.2018

Скрытый майнинг: хакеры атаковали компьютеры в России, Украине и Турции

Разработчики антивирусов рассказали о нападении ради «добычи» криптовалют (Сегодня).

Более 400 тысяч персональных компьютеров были атакованы в рамках попытки распространения вредоносного ПО для майнинга криптовалют. Хакеры использовали сложные трояны для заражения ПК в основном в России, но также в Турции, Украине и других странах, пишет News Bitcoin.

Комплексное вредоносное ПО пыталось противостоять антивирусной защите более 12 часов 6 марта. По данным Microsoft, большинство атакованных компьютеров – 73 %, находились в России, 18 % – Турции, 4 % – в Украине. Другие страны также пострадали.

«”Защитник Windows” заблокировал более 80 тысяч попыток нескольких сложных троянов, в которых были представлены передовые методы внедрения перекрестных процессов, механизмы устойчивости и методы обхода», – заявила исследовательская группа, разрабатывающая программное обеспечение Microsoft.

Более 400 тысяч пользователей подверглись нападению, сообщает Bleeping Computer. Исследователи утверждают, что идентифицировали атаку троянами на ранней стадии. Угроза была обнаружена с помощью антивирусной программы, которая начала блокировать дальнейшие попытки в течение нескольких минут.

Согласно команде разработчиков «Защитника Windows», вредоносная программа Dofoil пыталась проникнуть в процесс explorer.exe и внедрить вредоносный код. Затем другой explorer.exe должен был загрузить и запустить майнер криптовалют, замаскированный под файл Windows wuauclt.exe. Антивирусное программное обеспечение смогло обнаружить эти попытки, поскольку процесс выполнялся из другого места на жестком диске.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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