Updates on Our Security Work in Ukraine

By bdarwell

Published: 2022-02-28 · Archived: 2026-04-05 21:10:41 UTC

Read Ukrainian translation. Read Russian translation.

- **We took down a network run by people in Russia and Ukraine targeting Ukraine for violating our policy against coordinated inauthentic behavior. They ran websites posing as independent news entities and created fake personas across social media platforms including Facebook, Instagram, Twitter, YouTube, Telegram and also Russian Odnoklassniki and VK.**
- **In the past few days, we've seen increased targeting of people in Ukraine, including Ukrainian military and public figures by Ghostwriter, a threat actor that has been tracked for some time by the security community.**
- **We continue to roll out privacy and security measures to help people in Ukraine and Russia protect their accounts from being targeted.**

In response to Russia's invasion of Ukraine, our teams have been on high alert to identify emerging threats and respond as quickly as we can. Here are a few updates on our security work.

Coordinated Inauthentic Behavior

In the last 48 hours, we uncovered a relatively small network of about 40 accounts, Pages and Groups on Facebook and Instagram. They were operated from Russia and Ukraine and targeted people in Ukraine across multiple social media platforms and through their own websites. We took down this operation, blocked their domains from being shared on our platform, and shared information with other tech platforms, researchers and governments. When we disrupted this network on our platform, it had fewer than 4,000 Facebook accounts following one of more of its Pages and fewer than 500 accounts following one or more of its Instagram accounts.

This network used fake accounts and operated fictitious personas and brands across the internet — including on Facebook, Instagram, Twitter, YouTube, Telegram, Odnoklassniki and VK — to appear more authentic in an apparent attempt to withstand scrutiny by platforms and researchers. These fictitious personas used profile pictures likely generated using artificial intelligence techniques like generative adversarial networks (GAN). They claimed to be based in Kyiv and posed as news editors, a former aviation engineer, and an author of a scientific publication on hydrography — the science of mapping water. This operation ran a handful of websites masquerading as independent news outlets, publishing claims about the West betraying Ukraine and Ukraine being a failed state.

Our investigation is ongoing, and so far we've found links between this network and another operation we removed in April 2020, which we then connected to individuals in Russia, the Donbass region in Ukraine and two media organizations in Crimea — NewsFront and SouthFront, now sanctioned by the US government.

Hacking Attempts by Ghostwriter

In the past several days, we've seen increased targeting of people in Ukraine, including Ukrainian military and public figures by Ghostwriter, a threat actor that has been tracked for some time by the security community.

Ghostwriter typically targets people through email compromise and then uses that to gain access to their social media accounts and post disinformation as if it's coming from the legitimate account owners. We detected attempts to target people on Facebook to post YouTube videos portraying Ukrainian troops as weak and surrendering to Russia, including one video claiming to show Ukrainian soldiers coming out of a forest while flying a white flag of surrender. We've taken steps to secure accounts that we believe were targeted by this threat actor and, when we can, to alert the users that they had been targeted. We also blocked phishing domains these hackers used to try to trick people in Ukraine into compromising their online accounts.

Account Security

We're recommending that people in Ukraine and Russia take steps to strengthen the security of their online accounts to protect themselves from being targeted by threat actors.

We encourage people to use caution when accepting friend requests and opening links and files from people they don't know. Please refrain from reusing the same passwords across different services to prevent malicious hackers from gaining access to your information. We also strongly recommend using two-factor authentication on all online accounts.

Earlier this week, we rolled out additional privacy and security protections in Ukraine. We're now adding them in Russia as well, in response to public reports of targeting of civil society and protesters.

- **Lock Your Profile:** This tool allows people to lock their Facebook profile in one step. When someone's profile is locked, people who aren't their friends can't download, enlarge or share their profile photo, nor can they see posts or other photos on someone's profile, regardless of when they posted it. Our teams are working with civil society organizations to help ensure people know these tools are available.
- **Friends Lists:** We're temporarily removing the ability to view and search the friends lists of Facebook accounts to help protect people from being targeted.
- **Instagram Privacy and Security Reminders:** On Instagram, we're sending everyone in Russia a notification at the top of feed about privacy and account security. For public accounts, we are reminding people to check their settings in case they want to make their accounts private. When someone makes their account private, any new followers will need to be approved, and only their followers will be able to see their posts and stories. For people who already have private accounts, we're sharing tips on how to keep their account secure through strong passwords and two-factor authentication.

We continue to add measures to help protect people's privacy and security and will share these updates publicly. Read more about Meta's ongoing efforts regarding Russia's invasion of Ukraine.

Ukrainian Translation

Актуальна інформація щодо наших дій у зв'язку з забезпеченням безпеки в Україні

Натаніель Глейхер, керівник відділу політики безпеки та Девід Агранович, директор відділу запобігання загрозам

- **Через скоординовану неавтентичну поведінку ми видалили мережу сторінок у Facebook та Instagram, які контролювалися з території Росії та України Адміністратори цих сторінок керували веб-сайтами, видаючи себе за незалежні ЗМІ, та створювали фальшиві облікові записи в багатьох соціальних мережах, таких як Facebook, Instagram, Twitter, YouTube, Telegram, Одноклассники та Вконтакті.**
- **В останні декілька днів ми виявили посилення атак Ghostwriter на людей в Україні. Ghostwriter – це злочинна кіберорганізація, яка вже деякий час відстежується спільнотою безпеки. Під загрозою також опинились українських військові та громадські діячі.**
- **Щоб допомогти людям в Україні та Росії захистити свої облікові записи від атак зловмисників, ми продовжуємо впроваджувати заходи щодо конфіденційності та безпеки**

У відповідь на вторгнення Росії в Україну наша команда знаходиться в стані підвищеної готовності, щоб якнайшвидше виявляти загрози та реагувати на них. Ось кілька актуальний інформацій щодо нашої роботи в сфері безпеки:

Скоординована неавтентична поведінка

Протягом останніх 48 годин ми виявили відносно невелику мережу, що складалася з приблизно 40 облікових записів, сторінок та груп у Facebook та Instagram. Вони спрямовували інформацію до українців за допомогою соціальних мереж та власних веб-сайтів, які контролювалися з території Росії та України. Ми припинили діяльність вище згаданоЇ мережі, заблокували доступ до наших домен та поділилися інформацією з іншими технологічними платформами, дослідниками та урядами. Облікові записи, що входили до цієї мережі, на момент блокування мали близько 4 000 підписників на Facebook і 500 на Instagram.

Щоб здаватися більш автентичною, ця мережа використовувала фальшиві облікові записи і керувала неіснуючими особами та брендами в на різноманітних платформах,у тому числі в Facebook, Instagram, Twitter, YouTube, Telegram, Одноклассниках і Вконтакті. Фотографії цих профів були ймовірно створені за допомогою методів штучного інтелекту, таких як ГЗМ — генеративні змагальні мережі.

Вони стверджували, що знаходяться у Києві і видавали себе за колишнього авіаційного інженера, автора наукової публікації з гідрографії та редакторів новин. Вони запустили кілька веб-сайтів, щоб вдавати незалежні інформаційні агентства та публікувати заяви про те, що Захід зрадив Україну, а Україна є недодержавою.

Наше розслідування триває, і на даний момент ми виявили зв'язки між цією мережею та іншою, котру ми видалили в квітні 2020 року. Ми також з'ясували, що вона пов'язана з окремими особами, які перебувають

на територіЇ Росії та Донбасу в Україні, а також з двома медіа організаціями в Криму – NewsFront і SouthFront, які зараз знаходяться під санкціями уряду США.

Спроби хакерських атак з боку Ghostwriter

В останні кілька днів стали частішими атаки Ghostwriter на людей в Україні, включаючи українських військових і громадських діячів. Ghostwriter – це злочинна кіберорганізація, яка вже деякий час відстежується спільнотою безпеки.

Ghostwriter зазвичай націлюється на людей через компрометацію електронної пошти, а потім використовує ці дані для отримання доступу до їхніх облікових записів в соціальних мережах та поширює дезінформацію від їхнього імені. Ми виявили спроби таких атак на користувачів Facebook. Метою атак було розміщення відеороликів на YouTube, які показують, що українські війська є слабкими і що вони здаються у полон Росії. В одному з таких роликів стверджувалося, що українські солдати виходять з лісу під білим прапором для капітуляції.

Ми вжили заходів щодо захисту облікових записів, які, на нашу думку, стали жертвами атак цієї кіберорганізації.Також, по можливості, ми інформували користувачів про те, що вони стали мішенню хакерів. Ми заблокували фішингові домени, які хакери використовували для того, щоб обманом змусити людей в Україні скомпрометувати свої облікові записи в інтернеті.

Безпека облікових записів

Ми рекомендуємо жителям України і Росії зробити кроки для зміцнення безпеки своїх облікових записів в інтернеті, щоб захистити себе від атак кібер-зловмисників.

Ми закликаємо людей проявляти обережність при прийнятті запитів на додавання в друзі та відкритті посилань чи файлів від незнайомих людей. Будь ласка, утримайтеся від повторного використання однакових паролів в різних сервісах, щоб зловмисники не змогли отримати доступ до вашої приватної інформації. Ми також наполегливо рекомендуємо використовувати двофакторну аутентифікацію для всіх облікових записів в інтернеті.

На цьому тижні ми впровадили додаткові заходи щодо конфіденційності та безпеки користувачів в Україні. У відповідь на переслідування звичайного цивільного населення та протестуючих ми додамо їх також і в Росії.

- **Закритий профіль:** ця функція дозволяє користувачам закрити свій власний профіль на Facebook одним кліком. Якщо профіль буде закритим, відвідувачі Вашої сторінки Facebook, які не були додані як друзі, не матимуть змоги завантажувати, збільшувати чи ділитися фотографією Вашого профілю, а також бачити Ваші публікації чи інші фотографії, незалежно від того, коли вони були додані. Наша команда працює з недержавними та суспільними громадськими організаціями, щоб допомогти людям дізнатися про наявність цих функцій.

- **Списки Друзів:** в Україні ми тимчасово заблокували можливість переглядати та шукати списки друзів з метою захисту наших користувачів.

- **Сповіщення про забезпечення конфіденційності і безпеки в Instagram:** в Росії ми надсилаємо всім користувачам Instagram сповіщення зверху стрічки про конфіденційність та безпеку облікового запису. Також ми просимо людей, які мають відкриті облікові записи, перевірити свої налаштування, у випадку, якщо вони хочуть зробити свій профіль приватним. Приватні акаунти в Instagram мають змогу схвалювати або відхиляти запити на підписку. Лише схвалені особи мають змогу бачити публікації та Stories даного користувача. Для осіб у яких аккаунт вже є приватним, ми приготували порадами про те, як захистити свій профіль за допомогою надійних паролів та двоетапної аутентифікації.

Ми продовжимо впроваджувати додаткові заходи, які допоможуть захистити безпеку і приватність людей. Також ми публічно будемо ділитися інформацією про наші наступні оновлення. Дізнайтеся більше про зусилля Meta у зв'язку з вторгненням Росії в Україну.

Russian Translation

Последние новости о нашей работе в Украине по обеспечению безопасности пользователей

Натаниэль Глейчер, глава политики безопасности, и Давид Агранович, директор, предотвращение угрозами

- **Мы удалили сеть аккаунтов, страниц и груп, нацеленных на Украину, управляемую из Украины и России, за нарушение нашей политики против скоординированного недостоверного поведения. Они управляли веб-сайтами, выдавая себя за независимые новостные организации, и создавали фейковые личности на многих платформах социальных сетей, включая Facebook, Instagram, Twitter, YouTube, Telegram, "Одноклассники" и Vkontakte.**
- **В последние несколько дней мы наблюдаем усиление атак на людей в Украине, включая украинских военных и общественных деятелей, со стороны Ghostwriter – источника угроз, который уже некоторое время отслеживается сообществом безопасности.**
- **Мы продолжаем внедрять меры по обеспечению конфиденциальности и безопасности, чтобы помочь жителям Украины и России защитить свои аккаунты от атак.**

В ответ на вторжение России в Украину наши команды находятся в состоянии повышенной готовности, чтобы выявлять возникающие угрозы и реагировать на них как можно быстрее. Вот несколько обновлений о нашей работе в области безопасности.

Скоординированное недостоверное поведение

За последние 48 часов мы обнаружили относительно небольшую сеть из примерно 40 аккаунтов, страниц и групп в Facebook и Instagram. Они управлялись из России и Украины и были нацелены на людей в Украине через различные платформы социальных сетей и собственные веб-сайты. Мы пресекли эту операцию, заблокировали их домены на нашей платформе и поделились информацией с другими технологическими платформами, исследователями и правительствами. На момент остановки деятельности

этой сети на нашей платформе у нее было менее 4 000 аккаунтов в Facebook, которые были подписаны на одну или несколько ее страниц, и менее 500 аккаунтов, которые были подписаны на один или несколько ее аккаунтов в Instagram.

Эта сеть использовала поддельные аккаунты, управляла фейковыми личностями и брендами в интернете – в том числе в Facebook, Instagram, Twitter, YouTube, Telegram, “Одноклассниках” и Vkontakte – чтобы казаться более подлинными в очевидной попытке противостоять проверке со стороны платформ и исследователей. Эти фиктивные личности использовали фотографии профилей, вероятно, созданные с помощью методов искусственного интеллекта, таких как генеративные состязательные сети (GAN). Они утверждали, что находятся в Киеве, и выдавали себя за редакторов новостей, бывшего авиационного инженера и автора научной публикации по гидрографии – науке о картографировании воды. Эта операция запустила несколько сайтов, маскирующихся под независимые новостные издания, которые публиковали утверждения о том, что Запад предал Украину, а Украина является несостоявшимся государством.

Наше расследование продолжается, и на данный момент мы обнаружили связи между этой сетью и другой операцией, которую мы пресекли в апреле 2020 года, и которую мы затем связали с отдельными лицами в России, в регионе Донбасса, Украине и двумя медиаорганизациями в Крыму – NewsFront и SouthFront, которые сейчас находятся под санкциями правительства США.

Попытки хакерских атак группы Ghostwriter

В последние дни мы видели, что хакерская группа Ghostwriter осуществляет усиленные попытки организации атак на людей из Украины, в том числе на военных и общественных деятелей. Индустрия экспертов по безопасности уже на протяжение определенного времени отслеживает действия этой группы.

Обычно Ghostwriter начинает со взлома электронной почты, а затем использует ее для захвата учетных записей в социальных сетях и распространения дезинформации от лица владельцев аккаунтов. Мы обнаружили попытки атак на людей в Facebook для публикации на YouTube видео, показывающих украинские войска в ослабленном состоянии и готовых сдаться России. В том числе замечено видео, в котором якобы украинские солдаты выходят из леса под белым флагом капитуляции. Мы предприняли шаги для защиты учетных записей, которые, по нашему мнению, стали мишенью злоумышленников. Мы также, по возможности, предупреждали пользователей о том, что они подверглись атаке. Мы также заблокировали фишинговые домены, которые использовали хакеры, чтобы обманным путем заставить людей в Украине скомпрометировать свои собственные аккаунты.

Безопасность аккаунтов

Мы рекомендуем жителям Украины и России принять меры по усилению безопасности своих учетных записей в Интернете, чтобы защититься от направленных на них атак.

Мы рекомендуем людям проявлять осторожность при одобрении запросов на добавление в друзья и открывании ссылок и файлов от незнакомых людей. Пожалуйста, воздержитесь от повторного использования одних и тех же паролей в различных службах, чтобы злоумышленники не смогли получить

доступ к вашей информации. Мы также настоятельно рекомендуем использовать двухфакторную аутентификацию для всех учетных записей в интернете.

Ранее на этой неделе мы ввели дополнительные меры защиты конфиденциальности и безопасности на своих платформах для пользователей в Украине. Теперь, в ответ на публичные сообщения о преследовании гражданского общества и протестующих, мы запускаем следующие функции в России.

- **Закрыть свой профиль:** Этот инструмент позволяет людям закрыть свой профиль в Facebook в один клик. Когда профиль закрыт, люди, не являющиеся друзьями владельца аккаунта, не могут загрузить и увеличить фотографию профиля, или поделиться ею. Они также не могут видеть сообщения или другие фотографии на профиле пользователя, независимо от того, когда он их разместил. Наши команды работают с неправительственными и гражданскими организациями, чтобы помочь людям узнать, что эти инструменты доступны.
- **Списки друзей:** Мы временно убрали возможность просматривать списки друзей и искать в них контакты в аккаунтах Facebook в России, чтобы защитить людей от преследования.
- **Напоминания о конфиденциальности и безопасности в Instagram:** Мы отправляем всем пользователям Instagram в России уведомления в верхней части ленты о конфиденциальности и безопасности аккаунтов. Мы напоминаем открытым аккаунтам о необходимости зайти в настройки, если они хотят сделать свой аккаунт приватным. Если кто-то сделает свой аккаунт приватным, все новые подписчики должны будут получить одобрение, и только после получения одобрения смогут видеть сообщения и истории аккаунта. Для тех, у кого уже есть приватные аккаунты, мы делимся советами о том, как обеспечить безопасность аккаунта с помощью надежных паролей и двухфакторной аутентификации.

Мы продолжаем принимать меры по защите конфиденциальности и безопасности людей и будем публично делиться этими обновлениями. Читайте подробнее о текущих усилиях Meta в связи с вторжением России в Украину.

Source: https://about.fb.com/news/2022/02/security-updates-ukraine/