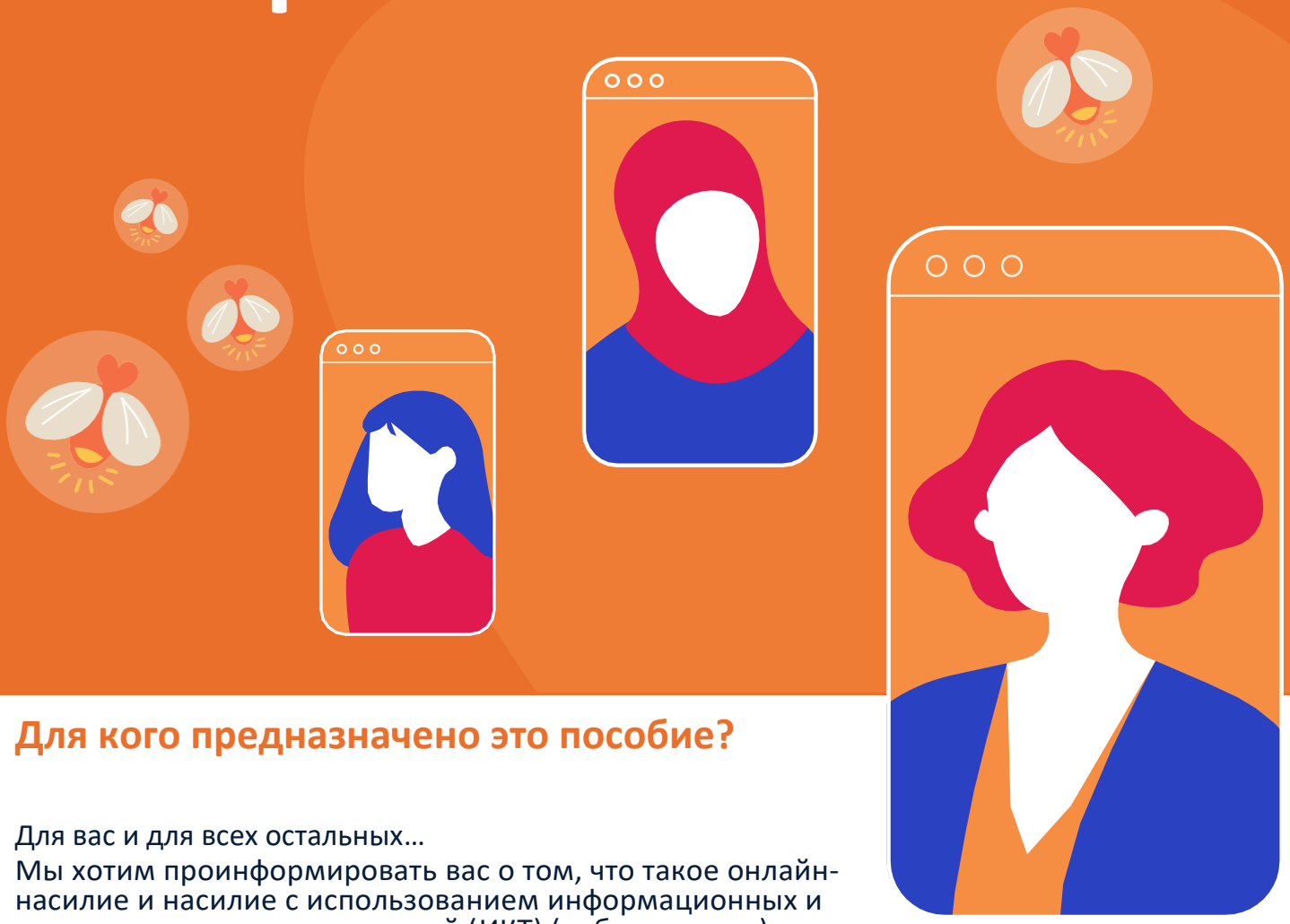
Sweden
Sverige

UN WOMEN

Пособие по противодействию гендерному кибернасилию



Для кого предназначено это пособие?

Для вас и для всех остальных…
Мы хотим проинформировать вас о том, что такое онлайн-насилие и насилие с использованием информационных и коммуникационных технологий (ИКТ) (кибернасилие), и предоставить вам пособие по тому, как их можно взять под контроль в цифровой среде.

@UNWomenTurkey

Начнем с определений?

Насилие в отношении женщин является одной из форм дискриминации в отношении женщин и нарушением прав человека, подпадающих под действие Конвенции о ликвидации всех форм дискриминации и других международных и региональных документов. Оно включает в себя гендерное насилие в отношении женщин, то есть насилие, направленное против женщин по той причине, что они являются женщинами, и/или такое, которое в непропорционально большой степени затрагивает женщин[1].

Таким образом, определение онлайн-насилия в отношении женщин распространяется на любой акт гендерного насилия в отношении женщин, который совершается, поддерживается или усугубляется частично или полностью в результате использования ИКТ, например мобильных телефонов и смартфонов, Интернета, платформ социальных сетей или электронной почты; в отношении женщины, поскольку она является женщиной, или в непропорционально большой степени затрагивает женщин.

Терминология в сфере борьбы с насилием в Интернете/насилием с применением ИКТ все еще разрабатывается, и в настоящее время нет его всеобъемлющего глобального определения и данных. В этом пособии мы используем термин «кибернасилие».

Тот факт, что насилие происходит в цифровой среде, не уменьшает тяжести этого преступления!

Как и все другие формы гендерного насилия, кибернасилие является нарушением прав человека и результатом неравенства!

Во всем мире неравенство во время пандемии усугубилось, и количество случаев кибернасилия как одной из форм гендерного насилия также возросло[2]

Кто подвергается кибернасилию?

Каждый!

Однако, поскольку причинами кибернасилия являются те же структуральные неравенства и дискриминация, что лежат в основе гендерного насилия, то женщины и девочки с большей вероятностью подвергаются кибернасилию и более серьезно страдают от него.

Согласно оценкам, в ЕС 23 процента женщин сообщили о том, что они хотя бы раз в жизни подвергались абьюзу или домогательствам в Интернете, и каждая десятая женщина с 15-летнего возраста сталкивалась с той или иной формой насилия в Интернете[3].

Женщины сталкиваются с риском подвергнуться кибернасилию, а также множественным и пересекающимся формам дискриминации по признаку образования, возраста, профессии, гендерной идентичности, сексуальной ориентации, этнической и расовой принадлежности или статуса родства.

Женщины, более заметные в цифровой среде, больше подвергаются кибернасилию[4]: женщины-политики, журналистки, художницы, писательницы, ученые и/или активистки в любой момент могут стать непосредственными мишенями лиц, совершающих киберпреступления.

Молодые люди, которые наиболее активны в цифровой среде, особенно подвержены кибернасилию.

Мы знаем, что 94% молодежи в возрасте 15–24 лет пользуются Интернетом[5].

Согласно опросу ЮНИСЕФ, проведенному среди миллиона молодых людей, более 70% молодежи в глобальном масштабе сталкиваются с кибернасилием[6].

В Турции лицам, наиболее подверженным кибернасилию, от 25 до 40 лет[7].

Кто совершает кибернасилие?

Лицом, совершающим кибернасилие, может быть бывший или нынешний супруг/партнер, сосед, коллега/ровесник, родственник или совершенно незнакомый человек.

Мы не виноваты в кибернасилии! Это преступление, которое должно быть наказуемо!

Хотя преступники используют разные тактики и инструменты, все они преследуют одну цель:

смутить, унизить, напугать, запугать, заставить замолчать или спровоцировать линчевание или злонамеренные нападки…

Как и откуда появляется кибернасилие?

Акты кибернасилия совершаются с использованием информационных и коммуникационных технологий, таких как платформы социальных сетей, приложения для обмена сообщениями и другие приложения, форумы, чаты игр, электронная почта и т. д.

Преступники, как правило, полны решимости сохранять контроль, и технологии являются лишь одним из многих инструментов, которые они используют для этой цели.

Если вы думаете, что у преступника есть много информации о вас, он(а) мог(ла) получить эту информацию, отслеживая ваши устройства, получив доступ к вашим аккаунтам, отследив ваше местоположение или собирая информацию о вас, доступную онлайн.

Давайте рассмотрим эту тему на нескольких примерах…

У кибернасилия много проявлений. Здесь приведены некоторые примеры:

Одной из разновидностей является **кибер-преследование.** Его также называют «сталкингом», и иногда это совсем не невинное времяпрепровождение.

Кибер-преследование представляет собой нежелательное наблюдение или слежку за кем-то с использованием ИКТ, а именно Интернета или других электронных приложений и платформ, и представляет собой модель поведения, которая причиняет вред или сильный стресс.

За нашими действиями могут наблюдать и следить через шпионские программы, такие как «клавиатурные перехватчики» или кейлоггеры – шпионское программное обеспечение, которое записывает каждое нажатие клавиши, сделанное пользователем, без нашего ведома об этом.

Другим часто встречающимся проявлением являются **онлайн-домогательства.** Приведем лишь несколько примеров:

- распространение нежелательных электронных писем и сообщений сексуального содержания;
- неприемлемые и агрессивные сообщения на цифровых платформах, угрозы физического и/или сексуального насилия.

Другим проявлением, часто встречающимся в детском и подростковом возрасте, является **онлайн-травля или кибербуллинг**.

Кибербуллинг — это травля с применением цифровых технологий. Она может происходить в соцсетях, платформах для обмена сообщениями или игр, в мобильных телефонах. Это – повторяющееся поведение, целью которого является запугать, вызвать гнев или опозорить тех, на кого оно направлено[8].

Другим проявлением с наиболее тяжкими последствиями является **распространение изображений каких-либо лиц без их согласия.**

Распространение изображений без согласия – это распространение онлайн фото- и видеоматериалов сексуального характера без согласия лиц, изображенных на этих материалах.

Как правило, правонарушителем является бывший супруг или партнер, получивший фотографии или видеоматериалы в период отношений. Эти изображения могут использоваться как угроза, чтобы не прекращать отношения или для каких-то иных требований. Преступники не обязательно должны быть бывшими супругами или партнерами, абсолютно незнакомый человек может получить доступ к нашим компьютерам/аккаунтам и использовать наши изображения для осуществления угроз.

Доступ к нашим личным данным без нашего согласия (взлом наших личных аккаунтов, кража паролей и т. д.) является **посягательством на частную жизнь.**

Приведем несколько примеров:

- Получение доступа к нашим фото и видео без нашего согласия или получение, использование,манипуляции и распространение таких материалов,
- Запись и распространение частной информации и контента, в т. ч. (сексуальных) изображений, аудиозаписей, видеозаписей без нашего информирования и согласия,
- Создание профиля от нашего лица с использованием нашей личной информации, также известное как «кэтфишинг»,
- Поиск, сбор и публикация нашей личной информации без нашего разрешения и согласия, также известная как «доксинг»,
- Обращение к нашим родственникам, друзьям, коллегам, чтобы добраться до нас, поставить нас в неловкое положение и оскорбить их.

Каковы последствия кибернасилия?

Когда мы сталкиваемся с кибернасилием, мы можем испытывать «гнев, замешательство, беспомощность, слабость, озабоченность по поводу нашей личной безопасности, страх и печаль», или можем опасаться, что «наша семья и друзья могут узнать об этом».

Мы можем умалять значение насилия, которое мы испытали, обвинять себя или решить, что с насилием ничего нельзя сделать и ситуацию никак не изменить. Мы можем даже удалить наши аккаунты в соцсетях или вообще отказаться от использования Интернета.

Удаление аккаунтов в соцсетях может казаться малозначительным, но оно вытесняет женщин и девочек за пределы цифрового пространства. Каждый человек имеет право чувствовать себя свободно и безопасно в общественных, частных и цифровых пространствах.

Замешательство и состояние, когда мы не знаем, что делать, вполне нормальны.

В результате кибернасилия женщины, как правило, испытывают страх, тревогу и депрессию, что приводит к их выходу из сетевой среды. Это часто сказывается на профессиональной деятельности и доходах лиц, подвергающихся насилию, и ограничивает их мобильность. Онлайн-формы насилия в отношении женщин и девочек связаны с психологическими, социальными и репродуктивными последствиями для их здоровья и могут сочетаться с физическим и сексуальным насилием в отношении жертв и пострадавших в оффлайн-среде.[9]

Как вы можете обеспечить свою безопасность?

Будучи мишенью онлайн-насилия, вы можете почувствовать, что всё вышло из-под контроля. Иногда вы можете вообще не хотеть ничего делать. Тем не менее, есть меры, которые вы можете принять, не обвиняя себя. Вот некоторые из них:

Верьте в себя!

Вы можете начать с ощущения уверенности в себе и определения того, что вы ощущаете как насилие.

Помните: это не ваша вина! Всегда напоминайте себе, что вы не должны винить себя, а насилию нет оправдания.

Чувства, потребности и действия, которые необходимо предпринять после эпизода насилия, у каждого человека могут быть разными!

Вы можете поделиться ими с кем-то, кому вы доверяете, и, возможно, обратиться за психологической консультацией...

Вы можете рассказать о том, что произошло и о ваших чувствах кому-то из друзей, членов семьи или людей, которым доверяете.

Именно вы лучше всех знаете, кому довериться.

Вы можете получить консультацию психологов, юристов или экспертов в области информационной безопасности.

Сделайте что-то, отчего вы чувствуете себя лучше!

Вы можете ежедневно уделять какое-то время себе и создать дистанцию между собой и онлайн-миром. Вы можете заняться чем-то приятным сами или друзьями.

Соберите доказательства!

Задокументируйте эпизоды кибернасилия, которым вы подверглись. Вам понадобятся эти доказательства, когда вы обратитесь к правовым методам борьбы. Также эти свидетельства могут помочь вам лучше оценить ваше состояние и заняться планированием вашей безопасности.

Не забывайте сохранять скриншоты. Еще лучше их распечатывать!

Если вы решили направить жалобу...

Вы должны знать, какие у вас есть права.

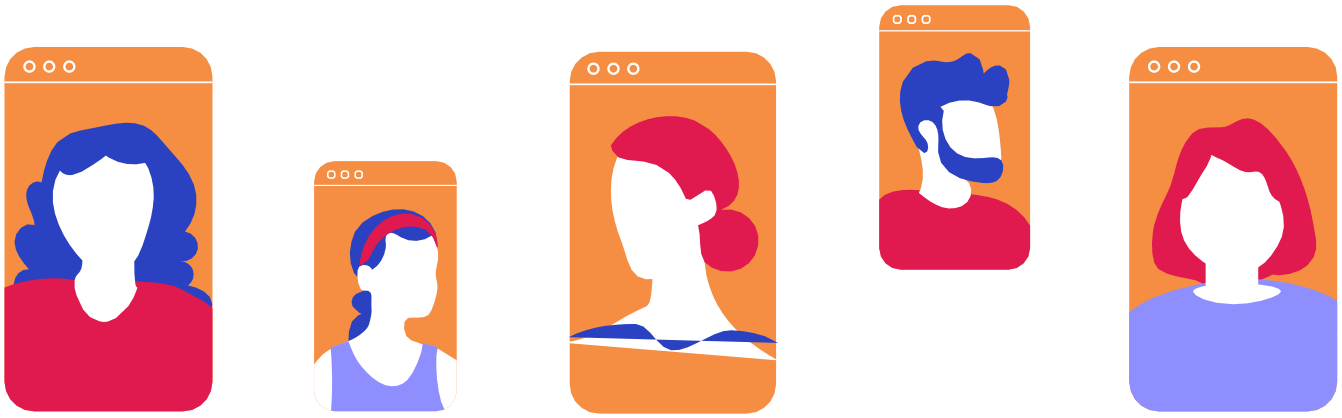
Вы можете побеседовать с юристами, занимающимися подобными делами, или с женскими консультационными центрами/комиссиями коллегий адвокатов, чтобы ознакомиться с юридическими процедурами.

Вы можете подать заявление в правоохранительные органы или прокуратуру. Убедитесь, что все соответствующие доказательства собраны заранее.

Если вы решите сообщить об этом соответствующим властям, попросите доверенное лицо сопровождать вас в ходе этих процедур.

Если преступник является одним из ваших коллег, вы можете сообщить об этом в механизм подачи жалоб на вашем рабочем месте (совет по этике и т. д.). Убедитесь, что они обеспечат вашу конфиденциальность!

Помните, что защита ваших личных данных и неприкосновенности вашей частной жизни являются вашими основными правами!



Кибернасилие по гендерному признаку может представлять собой преступное деяние. Существуют определенные в национальных и международных законах механизмы, которые можно использовать для борьбы с гендерным кибернасилием.

Международные соглашения:

- **Конвенция о ликвидации всех форм дискриминации в отношении женщин (CEDAW)**
- **Конвенция Совета Европы о предотвращении и борьбе с насилием в отношении женщин и домашним насилием (Стамбульская конвенция)**
- **Конвенция о киберпреступности (Будапештская конвенция)**

Что вы можете сделать для цифровой безопасности…

Мы обретем контроль в цифровом мире!

Насколько надежны и защищены ваши пароли?

Периодически меняйте пароли и избегайте использования наиболее часто используемых и легко угадываемых в мире[10] паролей, таких как «12345».

Не делитесь в своих постах информацией, связанной с ответами на вопросы безопасности на цифровых платформах.

Использование одного и того же пароля на всех платформах также является пробелом в безопасности. Кроме того, ваши пароли — это личные данные, и вы не должны делиться ими со своими друзьями и членами семьи.

Пользуетесь ли вы механизмами подачи жалоб?

Если вы подверглись насилию в интернете, вы можете воспользоваться механизмом подачи жалоб той платформы, на которой произошел инцидент. Так вы можете добиться того, что цифровые платформы станут более безопасными как для вас, так и для всех остальных пользователей.

При использовании механизмов подачи жалоб необходимо быть внимательными, поскольку жалобу следует направлять по соответствующей теме/разделу, чтобы ее надлежащим образом рассмотрели. Например, если кто-то притворяется вами или кем-то, кого вы знаете, в Instagram и создал аккаунт, используя ваши/их фотографии, вы не должны подавать жалобу в разделе «Спам»; вместо этого вы должны выбрать вариант «Сообщить об аккаунте» (Report Account) и сначала отметить его как «Ненадлежащий» (Inappropriate), а затем подать жалобу в разделе «Кто-то притворяется кем-то другим» (It's pretending to be someone else), выбрав одно из следующих: «Мною/кем-то, кого я знаю/знаменитостью или общественным деятелем» (Me/Someone I know/A celebrity or public figure).

Вы установили настройки безопасности?

Вы можете выбрать лиц, уполномоченных просматривать адрес электронной почты или номер телефона, который вы даёте при регистрации в качестве участника цифровых платформ. Кроме того, вы также можете выбрать, следует ли показывать вас среди результатов поиска на платформе, на которую вы регистрируетесь. Вы можете даже отключить такие функции, как «распознавание лица» на определенных платформах.

Все, что вам нужно сделать, это изучить настройки безопасности платформы, на которую вы регистрируетесь. Когда вы регистрируетесь на платформе, вам лучше установить ваши настройки безопасности до того, как начать делиться чем-то на этой платформе.

Вы подключили двухфакторную идентификацию?

Многие цифровые платформы имеют функцию двухфакторной аутентификации. Если вы используете эту функцию, то каждый раз, когда новое устройство используется для входа в вашу учетную запись, вам высылается код. Это гарантирует, что вы безопасно входите в свои учетные записи при смене устройства или браузера.

Уделяете ли вы внимание вашей безопасности в общественных местах?

Когда вы находитесь в публичных местах, если возможно, используйте собственное Интернет-соединение вместо общих соединений, к которым могут также получить доступ незнакомцы. Вы можете даже предпочесть использовать свой мобильный телефон в качестве модема (точки доступа), когда вам необходимо подключение к Интернету для вашего компьютера.

Кроме того, когда вы входите в свой аккаунт на компьютере в общественных местах, не забудьте выйти из всех платформ и очистить свою историю в браузере.

Авторизованы ли вы третьими сторонами?

Проблемы с безопасностью могут возникнуть, если вы используете свои аккаунты с определенных платформ, чтобы войти в приложения на цифровых платформах или использовать какие-то функции этих приложений. К примеру, вам нужно создать новый профиль для платформы, на которую вы подписываетесь, вместо того чтобы войти при помощи вашего аккаунта в Google, Facebook или Twitter. Будет лучше, если вы проверите приложения третьих сторон, которые вы, возможно, авторизовали на этих платформах, и отключить авторизацию для тех из них, которые не являются необходимыми.

Вы делитесь информацией о вашем местонахождении?

Если вы считаете, что можете подвергнуться насилию, лучше не распространяйте информацию о вашем местонахождении.

Установлено ли на вашем устройстве приложение, которое вам не знакомо?

Проверьте свои телефон и компьютер и удалите все приложения, которые вы не устанавливали сами. Эти приложения на ваши устройства могли установить лица, следящие и наблюдающие за вами.

Вы уверены, что не попались на крючок?

Приходящие вам на электронную почту письма не всегда отправляются с добрыми намерениями. Вирусы, или, как их еще называют, вредоносное программное обеспечение – это программы, собирающие все данные с вашего компьютера в том случае, если вы кликнете на ссылку в письме или кликнете или загрузите приложение к такому письму.

Чтобы понять, сдержит ли письмо вредоносную программу, в первую очередь проверяйте e-mail адрес отправки и формат приложенного файла.

Проверьте, насколько вы информированы о проблеме фишинга:
https://phishingquiz.withgoogle.com

А вот что можно сделать для других!

- Вы можете оставить жалобу в соцсетях, если кибернасилию подверглись другие пользователи.
- Вы можете отправить сообщение с выражением поддержки знакомому или незнакомому человеку, подвергшемуся кибернасилию, чтобы они знали, что не одиноки.
- Преступником может оказаться кто-то знакомый. В этом случае, если вы чувствуете, что начинаете оправдывать его перед пострадавшими от насилия, пересмотрите свое мнение и никогда не забывайте, что насилию нет оправданий.
- Вы не должны симпатизировать или принимать язык вражды и сексистские взгляды, а также распространять их – делиться ими или делать репост.
- Получайте разрешение от людей, которых вы отмечаете (тэгаете) в своих постах. Вы не знаете о том, какие проблемы с безопасностью можете создать для тех, кого отмечаете на своих фото!

Начните с рассылки этого пособия вашим друзьям…

1 Управление Верховного комиссара по правам человека (2018). Отчет Специального докладчика по насилию в отношении женщин, его причинам и последствиям, по онлайн-насилию в отношении женщин и девочек с позиции прав человека. Доступно по ссылке: https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/SRWomenIndex.aspx

2 ООН-женщины (2020). Онлайн-насилие и насилие с использованием ИКТ в отношении женщин и девочек во время пандемии COVID-19

3 Агентство Европейского союза по основным правам (2014). Насилие в отношении женщин: опрос по всему ЕС, стр. 104.

4 IGF. (2015). Форум по вопросам управления Интернетом – Форум передовых практик в области предотвращения онлайн-абьюза и гендерного насилия в отношении женщин

5 МСЭ (2020) Международный союз электросвязи

6 ЮНИСЕФ (2019). День безопасного Интернета. ЮНИСЕФ призывает принять согласованные меры https://www.unicef.org/press-releases/safer-internet-day-unicef-calls-concerted-action-prevent-bullying-and-harassment

7 Microsoft (2019). Цифровой индекс цивилизованности/DCI

8 ЮНИСЕФ (2019). Кибербуллинг: что это и как его остановить https://www.unicef.org/turkey/siber-zorbal%C4%B1k-nedir-ve-nas%C4%B1l-%C3%B6nlenir

9 Backe EL, Lilleston P, McCleary-Sills J (2018) Сетевые индивиды, гендерное насилие: обзор научной литературы по кибернасилию.Violence Gender 5(3):135–145.

10 Teampassword (2019). 50 наихудших паролей 2019 года: https://www.teampassword.com/blog/top-50-worst-passwords-of-2019

Ссылки:

Temur, N. (2019). Toplumsal Cinsiyete Dayalı Siber Şiddet -Kadın Örgütleri için Rehber

İlkiz, P., Tekin, A. ve Temur, N. (2019). Avrupa Kadın Lobisi- #KadınınİnternetiKadınınHakkı / #HerNetHerRightsTürkiye Kampanyası Eğitim Materyalleri

Опубликовано Структурой «ООН-женщины».

Авторы: Nurcihan Temur, Pınar İlkiz

Данная публикация была подготовлена при щедрой поддержке Швеции через Шведское агентство по сотрудничеству в области международного развития (СИДА). Мнения, выраженные в этой публикации, являются мнениями автора (авторов) и необязательно отражают мнения Структуры «ООН-женщины», Организации Объединенных Наций, любой из связанных с ней организаций или официальную позицию Швеции.