Финансирование Европейского Союза

ERKINDIK QANATY
общественный фонд

INSTITUTE FOR WAR & PEACE REPORTING
IWPR
ИНСТИТУТ РЕПОРТАЖЕЙ ВОЙНЫ И МИРА

КАК ЗАЩИТИТЬ СЕБЯ В ИНТЕРНЕТЕ?

Практические рекомендации

КИБЕРБЕЗОПАСНОСТЬ

– это важный навык для любого человека в 21 веке. С ее помощью можно обезопасить себя от мошенников и ответить на современные вызовы. Правила очень просты, и они помогут вам оставаться в безопасности, ведь киберугрозы можно предотвратить, а решить их последствия практически невозможно.

ЧЕМ ЧЕК-ЛИСТ И БРОШЮРА БУДУТ ВАМ ПОЛЕЗНЫ?

Чек-лист пригодится вам для еженедельного или ежемесячного чек-апа всего, что касается интернета, начиная от безопасного доступа, сохранения личных данных и использования искусственного интеллекта.

В брошюре вы найдете подробное описание каждого пункта чек-листа, с дополнительными рекомендациями авторки Даны Маликовой для более тщательной работы с программами, вашими устройствами и физической безопасностью.

КОМУ ИМЕННО ОНИ БУДУТ ПОЛЕЗНЫ?

Всем! Главное условие: вами должно двигать желание чувствовать себя свободно в киберпространстве.

Чек-лист и брошюра будут полезны как обычному человеку, так и целым организациям, так как они базируются на основных принципах кибербезопасности и включают в себя актуальные рекомендации.

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ:

1. Общественный WI-FI может стать средством взлома вашего телефона или компьютера, если вы к нему подключитесь. Более того, мошенники часто создают похожую сеть, чтобы запутать человека, а после подключения к ней вы можете стать жертвой киберпреступления.

2. То же может произойти, если вы дадите пароль от своей сети WI-FI незнакомцам. Будучи в вашей сети, мошенники могут взломать все устройства, что к ней подключены.

3. Во время блокировок или для получения доступа к заблокированному сайту, вам нужно подключиться к проверенному VPN, так как некоторые из них могут украсть ваши данные. ExpressVPN, Private Internet Access, CyberGhost, NordVPN – лучшие сервисы 2024 года по версии vpnMentor.

4. Фишинг все еще один из самых эффективных способов взлома сети, телефона и компьютера. Если вы переходите по непроверенным ссылкам, то высока вероятность, что мошенники смогут получить доступ к вашим устройствам, украсть информацию и даже оформить кредиты.

ЗАЩИТА ДАННЫХ:

1. Некоторые приложения просят от вас больше, чем дают вам. Например, калькулятор вдруг просит доступ к вашим контактам. Ему следует отказать, а лучше сразу удалить. У каждого приложения, которое вы скачиваете, есть политика конфиденциальности – описание того, как и зачем приложение будет использовать ваши данные – не ставьте галочку сразу, прочтите их.

2. Лучше заплатить за приложение и быть уверенным в том, что оно безопасно и вовремя обновится. Обновления – важная часть работы всех приложений, например, Windows. Чаще всего в обновление специалисты вкладывают решения защиты и борьбы с новыми вирусами и кибератаками, чтобы вы были в безопасности.

3. Резервное копирование поможет вам не потерять данные, если компьютер вдруг сгорел или у вас украли телефон. Одну копию можно хранить в облаке, другую на флэшке, а важный документ – еще и распечатать в одном экземпляре.

4. Чтобы мошенники вас не шантажировали, лучше хранить «чувствительные» данные «под подушкой», то есть не делиться ими. Личные фото, ИИН, адрес, банковские реквизиты – ваши персональные данные и они дороже золота.

5. Пароль должен состоять минимум из 13 рандомных символов: цифр, строчных и заглавных букв, которые ничего не означают. Имена, клички и даты рождения – под запретом. Менять их следует каждые полгода, хранить, записанные на бумажке или в менеджере паролей, например, KeePass.

6. Двухфакторная аутентификация есть везде, в том числе и в Telegram – это дополнительный способ для входа в приложение или на сайт. Однако, важно не выбирать вариант с СМС, его легче взломать, лучше использовать push-уведомления, Google Authenticator или e-mail.

7. Все мессенджеры, кроме Signal, на данный момент очень легко взломать, что бы вам не обещал производитель. Поэтому делиться в них важными документами небезопасно. Никогда не отправляйте удостоверение личности и другие важные документы посредством WhatsApp.

8. Кроме того, Signal – самое безопасное приложение для звонков и переписок.

9. Важно не забывать, что пароль нужен не только на телефоне, но и на личном и рабочем ноутбуке. Если вы не блокируете ноутбук, когда оставляете его в офисе или в зале во время кофе-брейка, у посторонних может быть доступ ко всем данным.

10. Помимо технических навыков, знание казахстанского законодательства поможет вам чувствовать себя увереннее и безопаснее в интернете и в обычной жизни, когда поднимается вопрос защиты персональных данных и вашей частной жизни.

ЧТО НЕОБХОДИМО ДЕЛАТЬ С КОМАНДОЙ ДЛЯ ТОГО, ЧТОБЫ ОБЕЗОПАСИТЬ СЕБЯ И ВАШИХ УЧАСТНИКОВ?

1. Каждая организация должна ставить на первое место безопасность своих сотрудников и участников, именно поэтому все процессы должны начинаться и базироваться на политике конфиденциальности (по-другому ее называют политикой для защиты персональных данных). Для ее разработки можно привлечь специалистов или разработать ее совместно с командой, используя наработки других организаций.

2. Когда вы собираете данные ваших участников, основывайтесь на политике конфиденциальности. Во время сбора вы должны объяснить, зачем вы собираете именно эти данные (например, ФИО, ИИН, адрес, реквизиты и тд.), и получить согласие на сбор, обработку и их использование, например публикацию в отчете.

Не собирайте данные, которые не понадобятся в работе, просто «на всякий случай». Если вы не собираетесь приобретать билеты участникам, то вам скорее всего не понадобится ИИН.

3. Перед тем, как фотографировать или снимать видео участников на ваших мероприятиях, важно оповестить их и получить согласие на съемку и дальнейшую публикацию, если вы будете где-то их размещать. Если кто-то отказался, вы можете уточнить, что при обработке и публикации фотографий или видео, этого человека не будет видно.

4. Базовые инструменты и знания кибербезопасности – это важный навык современных сотрудников и сотрудниц. Однако угрозы «развиваются» и видоизменяются постоянно, поэтому сотрудникам будет полезно проходить обучение не реже раза в год. Таким образом, вы обезопасите вашу команду, так как допустить ошибку может каждый человек, а последствия могут распространиться на всю организацию.

ЗАЩИТА АВТОРСКОГО ПРАВА И НЕЙРОСЕТЬ:

1. Если не указать авторов текста, видео или фотографии, помимо этического вопроса, вы можете столкнуться с юридическими последствиями - досудебной претензией. Поэтому в идеале нужно сперва получить их разрешение в переписке, а затем указать имя у себя.

2. ИИ может быть использован для поиска вдохновения и идей, но не для написания важных документов, помните, что программы уже распознают тексты, сгенерированные нейросетью.

3. Дипфейки могут быть интересным развлечением, пока не затрагивают достоинство другого человека.

4. ИИ не самое безопасное средство для обработки данных, поэтому, если вы используете его, сперва обязательно их зашифруйте, хотя бы с помощью цифр или буквенных обозначений.

Эта публикация финансируется Европейским Союзом. Её содержание является исключительной ответственностью IWPR и не обязательно отражает точку зрения Европейского Союза.

kzuncensored.cabar.asia