**Действенные советы по цифровой безопасности для журналистов и блогеров**

Цифровая безопасность требует знаний, времени и усилий. Поэтому нередко ей пренебрегают. Но только до тех пор, пока не случится цифровая катастрофа и критически важные данные не будут утеряны безвозвратно. Зачастую это слишком дорогая цена за ошибку и небрежность. Защитить информацию проще, чем справиться с последствиями ее утери. Вот, что для этого нужно сделать:

1. **Используйте двухфакторную аутентификацию (2FA)**: Включите 2FA для всех ваших аккаунтов, особенно для электронной почты и социальных сетей. Это добавит дополнительный слой защиты к вашему паролю.

*Двухфакторная аутентификация* (2FA) — это метод защиты учетных записей, при котором ваши права на доступ к аккаунту нужно подтвердить двумя разными способами. Это увеличивает безопасность, поскольку злоумышленнику придется не просто украсть пароль, а каким-то образом узнать и данные для второго шага аутентификации.

*Вот как это работает:*

Первый фактор — это обычно то, что вы знаете: пароль или PIN-код.

Второй фактор — это код, отправленный на ваш телефон, отпечаток пальца или лицо.

*Зачем нужна двухфакторная аутентификация:*

* Увеличение безопасности: Даже если злоумышленник узнает ваш пароль, без второго фактора он не сможет получить доступ к вашему аккаунту.
* Защита от фишинга и других атак: Автоматические атаки или атаки по схеме фишинга часто направлены на похищение паролей. С 2FA даже перехваченный пароль не даст доступа к аккаунту без второго фактора.
* Соответствие требованиям безопасности: Многие индустрии и регулирующие органы требуют использования 2FA для дополнительной безопасности в связи с повышением рисков кибератак
1. **Сильные и уникальные пароли**: Создавайте сложные и уникальные пароли для каждого аккаунта. Используйте менеджер паролей для хранения и генерации паролей.

***Сильные и уникальные пароли*** — это такие пароли, которые обеспечивают хорошую защиту от попыток взлома. Вот характеристики сильного пароля:

*Длина:* Пароль должен быть как минимум из 12 символов. Чем длиннее пароль, тем сложнее его взломать.

*Сложность:* В пароле должны быть использованы буквы верхнего и нижнего регистра, цифры и специальные символы, такие как !, @, #, $ и т. д.

*Уникальность:* Пароль должен быть уникальным для каждой учетной записи. Не используйте один и тот же пароль для разных сайтов или приложений.

*Непредсказуемость:* Избегайте общих слов, фраз, дат рождения, последовательных чисел или клавиш клавиатуры (например, qwerty).

*Пример сильного пароля:* Gv3!rB\*9nF$l

***Слабые пароли*** обычно:

* + Короткие (меньше 8 символов).
	+ Простые или очевидные, например, password, 123456, qwerty, abc123.
	+ Содержат личную информацию, которую легко угадать, например, имя, дату рождения, имя домашнего животного и т.д.
	+ Используются на нескольких платформах и сайтах.

***Почему простые пароли легко взломать:***

*Словарные атаки:* Хакеры используют программы, которые автоматически пробуют миллионы популярных и общеизвестных слов и фраз. Если ваш пароль — обычное слово или популярная комбинация, его можно взломать за секунды.

*Атаки по методу "грубой силы" (brute-force attacks):* В этих атаках используются программы, которые перебирают все возможные комбинации букв, цифр и символов до тех пор, пока не будет найден правильный пароль. Короткие и простые пароли взламываются гораздо быстрее, чем длинные и сложные.

*Утечки данных:* Если хакеры получают доступ к базе данных с паролями, простые пароли легче всего угадать или расшифровать после утечки.

1. **Шифрование данных**: Шифруйте ваши устройства и данные. Используйте инструменты, такие как BitLocker для Windows или FileVault для macOS, чтобы зашифровать жесткий диск вашего компьютера.

***BitLocker и FileVault*** — это встроенные инструменты шифрования, предоставляемые соответственно Microsoft Windows и Apple macOS. Они предназначены шифрования всей информации на жестком диске. Так что если устройство будет украдено или утеряно, доступ к вашим данным все равно никто не получит.

***BitLocker для Windows***

*Как это работает:* BitLocker использует алгоритм шифрования AES и может быть настроен для использования 128- или 256-битного ключа. При включении BitLocker генерирует ключ шифрования, который затем защищается одним или несколькими методами аутентификации: TPM чип (Trusted Platform Module), PIN-код, стартовый ключ на USB-устройстве или комбинация этих методов.

*Как этим пользоваться:*

1. Откройте "Панель управления" > "Система и безопасность" > "Шифрование диска BitLocker".
2. Выберите диск для шифрования и следуйте инструкциям мастера настройки.
3. Сохраните восстановительный ключ в безопасное место.
4. Дождитесь завершения процесса шифрования.

***FileVault для macOS***

*Как это работает:* FileVault использует шифрование XTS-AES-128 с ключом шифрования 256-бит для полного шифрования диска. При включении FileVault пользователю будет предложено ввести свой пароль учетной записи, который используется для создания ключа шифрования. Ключи шифрования хранятся в зашифрованном виде и доступны только после аутентификации пользователя.

*Как этим пользоваться:*

1. Откройте "Системные настройки" > "Безопасность и конфиденциальность" > вкладка "FileVault".
2. Нажмите на замок в левом нижнем углу и введите пароль администратора.
3. Нажмите «Включить FileVault» и следуйте инструкциям на экране.
4. Запишите ключ восстановления и храните его в надежном месте.
5. Перезагрузите Mac, если это будет запрошено.

Использование BitLocker или FileVault значительно повышает безопасность данных на вашем устройстве. Однако всегда важно помнить о сохранности резервной копии восстановительных ключей, поскольку в случае их потери доступ к данным может быть необратимо утрачен.

1. **Безопасное соединение**: Используйте VPN (виртуальную частную сеть) для защиты вашего интернет-соединения, особенно когда вы используете общественные Wi-Fi сети.

VPN (Virtual Private Network — виртуальная частная сеть) — это технология, создающая защищенное интернет-соединение, путем шифрования вашего трафика и изменения вашего IP-адреса. VPN соединяет ваше устройство с сервером VPN-провайдера, и весь интернет-трафик передается через этот сервер. Трафик между вашим устройством и сервером VPN шифруется, что обеспечивает конфиденциальность и защиту данных.

***Для чего используется VPN?***

*Конфиденциальность и анонимность:* VPN скрывает ваш реальный IP-адрес и геолокацию, предоставляя вам анонимность в интернете. Это помогает защитить вашу личную информацию от хакеров и слежки.

*Безопасность на публичных Wi-Fi сетях:* Обеспечивает защиту ваших данных при использовании небезопасных публичных Wi-Fi сетей, защищая вас от возможных атак.

*Защита от слежки:* Защищает от слежки третьими сторонами.

***Как этим пользоваться?***

**-** Выберите надежного VPN-провайдера, который соответствует вашим потребностям в плане конфиденциальности, скорости и доступности серверов.

**-** Скачайте и установите VPN-клиент от вашего провайдера на ваше устройство. Большинство VPN-провайдеров предоставляют программы для различных устройств и операционных систем.

**-** В программе VPN выберите сервер, к которому хотите подключиться. Обычно можно выбрать страну или даже конкретный город.

**-** Активируйте VPN-соединение в программе. После подключения весь ваш интернет-трафик будет проходить через защищенный VPN-сервер.

1. **Осторожнее с вложениями и ссылками**: Не открывайте вложения или ссылки от неизвестных источников. Фишинговые атаки часто используют такие методы для установки вредоносного ПО.

***Фишинг*** — это вид кибератаки, при которой злоумышленники маскируются под доверенные источники или личности, чтобы украсть конфиденциальную информацию, такую как логины, пароли, данные банковских карт и другую личную информацию. Целью фишинга является обман пользователей с целью заставить их самих предоставить свои личные данные, перейти по вредоносной ссылке или скачать зараженный файл.

***Как это работает?***

*Создание фишингового сообщения:* Злоумышленники создают электронные письма, текстовые сообщения или сообщения в социальных сетях, которые выглядят как официальные уведомления от реальных организаций, таких как банки, крупные интернет-магазины, платежные системы и т.д.

*Маскировка:* Фишинговые сообщения часто содержат логотипы, шрифты и другие характеристики, имитирующие настоящие уведомления от этих организаций, чтобы их сложнее было отличить от подлинных сообщений.

*Привлечение жертв:* В сообщениях обычно содержится призыв к срочным действиям, таким как подтверждение учетных данных, изменение пароля или просмотр подозрительной активности.

*Вредоносные ссылки или вложения:* Письма содержат ссылки, которые перенаправляют пользователя на поддельные веб-сайты, либо вложения, которые могут заразить компьютер вредоносным ПО.

***Что обычно пишут в письмах, содержащих фишинговые ссылки?***

Фишинговые письма могут включать:

*Срочные уведомления:* "Ваш аккаунт временно заблокирован. Нажмите здесь, чтобы восстановить доступ."

*Предложения:* "Вы выиграли iPhone. Перейдите по ссылке, чтобы подтвердить адрес доставки."

*Предупреждения о безопасности:* "Мы обнаружили подозрительную активность на вашем аккаунте. Немедленно проверьте свои настройки безопасности."

*Просьбы о подтверждении личной информации:* "Подтвердите вашу учетную запись и пароль, перейдя по следующей ссылке."

*Призывы к действию:* "Ваша кредитная карта скоро истекает. Обновите свои платежные данные, чтобы продолжить сервис."

***Как защититься от фишинга?***

*Проверяйте отправителя:* Убедитесь, что адрес отправителя соответствует адресу организации. Остерегайтесь странных или незнакомых адресов.

*Избегайте перехода по подозрительным ссылкам:* Не кликайте по ссылкам в неожиданных или подозрительных письмах.

*Не раскрывайте личную информацию:* Никогда не предоставляйте свои конфиденциальные данные в ответ на электронные письма.

1. **Регулярное обновление ПО**: Убедитесь, что операционная система и все приложения на ваших устройствах регулярно обновляются. Патчи безопасности помогают защититься от известных уязвимостей.

Частота обновлений программного обеспечения зависит от нескольких факторов, включая производителя устройства, программное обеспечение и операционную систему. Обычно:

Операционные системы компьютеров (например, Windows, macOS) обновляются примерно каждые несколько месяцев с крупными обновлениями и чаще с безопасностными исправлениями или патчами.

Смартфоны обновляются похожим образом. Android и iOS получают крупные обновления раз в год, а обновления, связанные с повышением безопасности, могут выходить каждый месяц или даже чаще.

***Зачем нужно обновлять ПО?***

*Безопасность:* Обновления часто содержат патчи для уязвимостей, что помогает защитить устройство от вирусов и вредоносного ПО.

*Устранение ошибок:* Обновления часто исправляют известные ошибки и проблемы в программном обеспечении.

*Повышение производительности:* Обновления могут оптимизировать программное обеспечение для более быстрой и эффективной работы.

***Много ли места занимает обновление?***

Размер обновления зависит от конкретного обновления и устройства. Например:

Обновления операционной системы для компьютеров и смартфонов могут занимать от нескольких сотен мегабайт до нескольких гигабайт.

Приложения обычно требуют меньше места для обновления, но это также зависит от приложения и объема добавляемых изменений.

***Что будет, если отключить обновления?***

Отключение обновлений может иметь следующие последствия:

*Уязвимость к атакам:* Без последних патчей безопасности ваше устройство становится более уязвимым к новым вирусам и вредоносному ПО.

*Нарушение работы приложений:* Некоторые приложения могут требовать новейших версий операционных систем для правильной работы или для доступа к новым функциям.

*Проблемы совместимости:* Старое ПО может со временем стать несовместимым с новыми стандартами и технологиями, что может вызвать проблемы с подключением к сервисам или использованием аксессуаров.

1. **Антивирусное ПО**: Используйте надежное антивирусное программное обеспечение для защиты от вредоносного ПО и вирусов.

При выборе антивирусного программного обеспечения важно оценить несколько ключевых факторов, чтобы определить его надежность. Вот основные критерии, на которые стоит обратить внимание:

***Независимые тесты и рейтинги***

Самый надежный способ оценить эффективность антивируса — это изучить результаты независимых тестирований. Организации, такие как AV-Comparatives, AV-Test и Virus Bulletin, регулярно проводят тесты и публикуют результаты, оценивая антивирусы по таким параметрам, как:

*Эффективность обнаружения вирусов*: насколько хорошо ПО обнаруживает и удаляет вирусы.

*Влияние на производительность системы:* насколько антивирус замедляет компьютер.

*Ложные срабатывания:* как часто антивирус ошибочно помечает безопасные файлы как вредоносные.

***Особенности защиты***

Надежное антивирусное ПО должно предлагать комплексные функции защиты, включая:

*Реальное время сканирования:* обеспечивает непрерывную защиту, сканируя файлы при доступе.

*Защита от рансомвара:* предотвращает блокировку доступа к вашим данным через шифрование.

*Веб-защита:* блокирует вредоносные сайты и загрузки.

*Фаервол:* предотвращает несанкционированный доступ к вашей сети.

*Защита личной информации:* защищает чувствительные данные, такие как банковская информация.

***Поддержка и обновления***

Регулярные обновления важны для антивирусного ПО, чтобы оно могло защищать от последних угроз. Также важна качественная поддержка клиентов.

***Могут ли бесплатные антивирусы быть надежными?***

Многие бесплатные антивирусные программы могут быть достаточно надежными для обеспечения базовой защиты. Программы, такие как Avast Free Antivirus, AVG AntiVirus Free, и Bitdefender Free Edition, часто показывают хорошие результаты в независимых тестированиях. Однако важно понимать, что бесплатные версии обычно имеют ограниченные функции по сравнению с платными, и могут включать в себя рекламу или предложения обновиться до платной версии.

Для обычного домашнего использования хорошо подойдет бесплатный антивирус от известного производителя. Если же вы часто сталкиваетесь с конфиденциальной информацией или ваши устройства используются в коммерческих целях, рекомендуется рассмотреть платные решения с расширенными возможностями защиты.

1. **Физическая безопасность устройств**: Защитите свои устройства от физического доступа неавторизованными лицами. Используйте пароли на экране блокировки и не оставляйте устройства без присмотра в общественных местах.

Да, пароли на экране блокировки могут быть как надёжными, так и ненадёжными, аналогично паролям для входа в учётные записи онлайн. Важно выбирать надежные пароли для экрана блокировки, чтобы максимально защитить доступ к вашему устройству от несанкционированного доступа.

Собственно говоря, рекомендации по выбору пароля для экрана блокировки такие же, как и к любым другим паролям. Для выбора графических паролей есть еще несколько важных советов:

* + *Избегайте простых и очевидных паттернов при выборе графического пароля.* Наиболее распространённые паттерны, такие как буквы (L, S, Z), числа (0, 1, 2) или прямые линии, следует избегать. Эти паттерны легко угадать, так как они являются интуитивно понятными и часто используются.
	+ *Используйте максимальное количество точек.* Большинство устройств позволяют использовать от 4 до 9 точек для создания графического ключа. Чем больше точек вы используете, тем больше возможных комбинаций и тем сложнее угадать пароль.
	+ *Создавайте сложные и непредсказуемые узоры.* Используйте перекрёстные или зигзагообразные линии, которые пересекают или касаются друг друга в неочевидных точках. Это значительно усложняет попытки воспроизведения узора по памяти или по отпечаткам на экране.
	+ *Регулярно меняйте графический ключ.* Как и в случае с обычными паролями, регулярное изменение графического ключа поможет уменьшить риск его подбора или использования после возможного случайного его раскрытия.
	+ *Очищайте экран устройства.* Регулярно протирайте экран устройства, чтобы уменьшить видимость следов, которые могут быть оставлены при вводе графического ключа. Это помогает предотвратить возможность визуального восстановления вашего пароля посторонними.
	+ *Не делитесь своим графическим ключом.* Избегайте демонстрации вашего способа разблокировки устройства другим людям. Даже случайные наблюдатели могут запомнить или записать ваш паттерн.
1. **Использование защищенных приложений для общения**: Предпочитайте приложения с концом-к-концу шифрованием для переписки и звонков, такие как Signal или Telegram.

Чтобы понять, насколько надёжен мессенджер, важно рассмотреть несколько ключевых аспектов безопасности и конфиденциальности, предлагаемых этим приложением:

*Шифрование*

Одна из самых важных функций — это шифрование end-to-end. Это значит, что сообщения, файлы и звонки зашифрованы на устройстве отправителя и расшифровываются только на устройстве получателя. Посторонние, включая самого провайдера услуги, не могут прочитать или прослушать эти данные.

*Политика конфиденциальности и соблюдение приватности*

Важно изучить, как мессенджер обращается с вашими данными: собирает ли приложение метаданные (например, время и дату сообщений, контакты), как долго хранятся данные, и передаются ли данные третьим сторонам.

*Независимые аудиты и открытый исходный код*

Наличие независимых аудитов безопасности и открытого исходного кода может служить показателем прозрачности и надёжности приложения. Это позволяет независимым экспертам проверять безопасность и уязвимости программы.

***Последствия использования ненадёжного мессенджера:***

*Компрометация личной информации:* Слабо защищённое приложение может позволить хакерам доступ к вашим личным сообщениям, фотографиям, видео и другим файлам.

*Перехват и прослушивание сообщений:* Если мессенджер не использует шифрование end-to-end, злоумышленники могут перехватывать и читать ваши сообщения.

*Утечка данных:* Ненадёжные мессенджеры могут случайно или намеренно раскрывать ваши данные третьим лицам, включая рекламодателей.

***Возможность перехвата и подслушивания:***

*Текстовые сообщения и файлы:* Если используется шифрование end-to-end, перехватить и прочитать сообщения почти невозможно. Без этого шифрования сообщения могут быть уязвимы для перехвата.

*Голосовые сообщения и звонки:* Также защищены шифрованием end-to-end в надёжных мессенджерах. В противном случае их можно перехватить, особенно если злоумышленник имеет доступ к сети передачи данных.

***Наиболее безопасными мессенджерами считаются:***

*Signal*

Шифрование: Signal использует протокол шифрования end-to-end, разработанный Open Whisper Systems, который также используется в WhatsApp и других мессенджерах. Он шифрует сообщения, звонки, фотографии и видео.

Приватность: Signal не хранит данные о пользователях, за исключением времени регистрации и последнего времени входа в систему, и не собирает метаданные о том, кто с кем общается.

Открытый исходный код: Signal открыт для независимого аудита, что позволяет специалистам по безопасности регулярно проверять и улучшать его безопасность.

*WhatsApp*

Шифрование: WhatsApp предлагает шифрование end-to-end для всех видов коммуникации на своей платформе.

Приватность: Несмотря на высокий уровень шифрования, WhatsApp (принадлежит Facebook, теперь Meta) подвергался критике за способы обработки пользовательских данных и связь с Facebook, что вызывает опасения по поводу конфиденциальности.

*Telegram*

Шифрование: Telegram предлагает шифрование end-to-end в "секретных чатах", но его обычные чаты используют клиент-серверное шифрование, и серверы могут хранить сообщения.

Приватность: Telegram имеет функции, которые позволяют пользователям больше контролировать свою приватность, но его не всегда рекомендуют для высококонфиденциальной коммуникации из-за структуры его шифрования и хранения данных.

*Threema*

Шифрование: Threema шифрует все сообщения, звонки, файлы и статусы end-to-end.

Приватность: Threema придерживается строгой политики не хранения метаданных и позволяет пользователям использовать сервис анонимно без необходимости предоставления номера телефона.

*Wire*

Шифрование: Wire использует шифрование end-to-end для текстовых сообщений, файлов, звонков и видеозвонков.

Приватность: Wire публикует свои протоколы безопасности и регулярно проходит независимые аудиты. Он также позволяет регистрацию без использования личных данных, таких как номер телефона.

Выбор "самого безопасного" мессенджера зависит от вашей потребности в приватности, необходимости шифрования и доверия к компании, управляющей сервисом. Signal часто считается одним из лучших выборов для тех, кто ищет максимальную защиту конфиденциальности и безопасности.

1. **Осведомленность о цифровых угрозах**: Регулярно обучайтесь и следите за новостями в области кибербезопасности, чтобы быть в курсе новых угроз и методов защиты.

Получать свежую и актуальную информацию о новых цифровых угрозах на можно из разных источников. Например:

***Специализированные информационные порталы о кибербезопасности***

*Хабр (раздел кибербезопасности):* На Хабре публикуются статьи, блоги и новости от экспертов в области IT и кибербезопасности.

*SecurityLab:* Этот ресурс предоставляет новости, анализы и исследования в области информационной безопасности.

***Блоги крупных компаний по кибербезопасности***

*Блог Kaspersky на Дзен.ру:* Компания Касперского регулярно публикует анализы и новости о последних киберугрозах.

*Facebook аккаунт ESET NOD32:* ESET также делится новостями и исследованиями в области защиты от вирусов и киберугроз.

***Телеграм-каналы****:* Существует множество каналов в Телеграм, посвященных кибербезопасности, где регулярно публикуются обновления и новости.

В Telegram есть множество каналов, посвящённых кибербезопасности, где регулярно публикуется информация о последних угрозах, советы по защите и анализы инцидентов. Вот несколько популярных русскоязычных телеграм-каналов по этой теме:

*Kaspersky Daily* - Канал известной компании Касперский, где публикуются новости, статьи и аналитика по темам кибербезопасности.

*SecurityLab* - Телеграм-канал популярного портала SecurityLab, где публикуются актуальные новости кибербезопасности.

*Xakep.RU* - Канал известного журнала о хакинге и информационной безопасности, где обсуждаются последние новости, методы атак и защиты.

*РБК Технологии и Медиа* - Хотя не специализированный канал по кибербезопасности, регулярно включает новости и аналитику по актуальным темам безопасности.

*CyberSecInfo* - Этот канал предоставляет новости, статьи и аналитику о кибербезопасности, киберугрозах и защите данных.

1. **Резервное копирование данных**: Регулярно создавайте резервные копии важных данных на внешних носителях или в облачном хранилище. Это может помочь восстановить информацию в случае атаки или потери данных.

Выбор метода резервного копирования зависит от ваших конкретных нужд. Если вам нужно быстро и недорого скопировать небольшое количество данных, Flash-диск может быть хорошим выбором. Для регулярного резервного копирования большого объема данных лучше подходит внешний жесткий диск. Облачные хранилища идеально подходят для тех, кому важна возможность доступа к данным из разных мест и кто готов платить за дополнительные удобства и услуги.

Разные варианты хранения резервных копий имеют свои плюсы и минусы.

***Flash USB***

*Достоинства:*

Портативность: Flash-диски легкие и компактные, их удобно носить с собой.

Доступность: Они обычно стоят недорого и доступны в разных размерах хранения.

Простота использования: Легко подключаются к большинству компьютеров без дополнительного программного обеспечения.

*Недостатки:*

Ограниченное пространство для хранения: По сравнению с внешними жесткими дисками, Flash-диски предлагают меньший объем памяти.

Надежность: Flash-диски могут легко повредиться (физически или электронно), что может привести к потере данных.

Безопасность: Если Flash-диск потеряется, любой, кто его найдет, может получить доступ к данным, если они не зашифрованы.

***Внешний жесткий диск***

*Достоинства:*

Большой объем хранения: Внешние жесткие диски обычно имеют больший объем хранения по сравнению с Flash-дисками.

Цена за гигабайт: Обычно предлагают лучшую стоимость за гигабайт, чем Flash-диски.

Надежность: При правильном обращении могут быть более надежными для долгосрочного хранения.

*Недостатки:*

Портативность: Больше и тяжелее, чем Flash-диски.

Уязвимость к физическим повреждениям: Могут повреждаться при ударах или падениях.

***Облачное хранилище***

*Достоинства:*

Доступность с любого устройства: Доступ к файлам можно получить с любого устройства, подключенного к интернету.

Защита от физического повреждения: Данные хранятся на удаленных серверах, что уменьшает риск потери данных из-за физических повреждений вашего оборудования.

Масштабируемость: Объем хранения можно легко увеличить в зависимости от ваших потребностей.

*Недостатки:*

Зависимость от интернета: Доступ к данным возможен только при наличии интернет-соединения.

Проблемы конфиденциальности и безопасности: Ваши данные могут стать объектом кибератак или несанкционированного доступа, если провайдер облачных услуг не применяет должные меры безопасности.

Стоимость**:** За облачное хранилище обычно нужно платить регулярную подписку, в зависимости от объема занимаемого пространства и других услуг.

1. **Используйте безопасные файлообменники и облачные хранилища**: При работе с конфиденциальными источниками используйте платформы, предлагающие анонимные и зашифрованные способы передачи данных.

***Как выбрать безопасный файлообменник или облачное хранилище:***

*Шифрование:* Убедитесь, что сервис предлагает шифрование данных на всех этапах — как во время передачи (шифрование конца-к-концу), так и при хранении на серверах. Шифрование должно быть стандартом, например, AES с ключом не менее 256 бит.

*Политика конфиденциальности и соответствие стандартам:* Прочитайте политику конфиденциальности, чтобы понять, как сервис обрабатывает и защищает ваши данные. Желательно выбирать сервисы, соответствующие международным стандартам безопасности, таким как GDPR, HIPAA или ISO/IEC 27001.

*Двухфакторная аутентификация:* Поддержка двухфакторной аутентификации значительно повышает безопасность вашего аккаунта, защищая доступ к данным даже в случае утечки пароля.

*Репутация и отзывы:* Изучите отзывы пользователей и независимые оценки. Большой опыт работы и положительные отзывы пользователей могут быть хорошим показателем надёжности сервиса.

*Регулярные аудиты и обновления безопасности:* Проверьте, насколько часто провайдер проводит аудиты безопасности и обновляет свои системы для защиты от новых угроз.

***Риски использования небезопасных файлообменников и облачных хранилищ:***

*Доступ злоумышленников к данным:* Если сервис не использует должное шифрование, хакеры могут легко перехватить и получить доступ к вашим файлам.

*Потеря данных:* Ненадёжные сервисы могут столкнуться с техническими сбоями или нарушениями данных, что приведет к потере важной информации.

*Утечка конфиденциальной информации:* В случае неправильной обработки данных сервисом, ваша личная или конфиденциальная информация может быть случайно раскрыта или продана третьим лицам.

*Юридические риски:* Несоблюдение законодательных и отраслевых стандартов безопасности может привести к юридическим проблемам для вашего бизнеса или личным последствиям.

*Распространение вредоносного ПО:* Некоторые файлообменники могут быть источником вредоносного ПО, которое может быть автоматически загружено вместе с файлами.

1. **Осторожно с метаданными**: Фотографии и документы могут содержать метаданные, которые раскрывают местоположение, дату и время создания, информацию об устройстве и другие подробности. Используйте инструменты для их удаления перед публикацией или отправкой.

***Удаление метаданных из изображений и фотографий***

*Windows*: Вы можете использовать встроенный Проводник Windows для удаления метаданных. Кликните правой кнопкой мыши по файлу, выберите "Свойства", перейдите во вкладку "Подробно" и нажмите "Удалить свойства и личную информацию".

*macOS:* Можно использовать приложение "Просмотр" для удаления метаданных. Откройте изображение в "Просмотре", выберите "Инструменты" -> "Показать инспектора", перейдите на вкладку с информацией о файле (маленький "i") и удалите данные из раздела "EXIF".

***Удаление метаданных из документов Office***

*Microsoft Office:* Откройте документ, перейдите в "Файл" -> "Сведения" -> "Проверить наличие проблем" -> "Проверить документ", и затем выберите опции для удаления желаемых метаданных.

*LibreOffice*: Откройте документ, перейдите в "Файл" -> "Свойства", затем на вкладке "Общие" снимите галочку "Применять информацию о пользователе" и удалите оставшиеся метаданные.

***Удаление метаданных из PDF***

Используйте Adobe Acrobat: Откройте PDF, перейдите в "Файл" -> "Свойства", нажмите "Удалить метаданные" в диалоговом окне свойств.

* Существуют также сторонние инструменты и онлайн-сервисы, такие как Smallpdf или PDF24, которые могут помочь удалить метаданные из PDF-файлов.

***Восстановление метаданных***

Обычно, после удаления метаданных из файла, их восстановление без предварительного создания резервной копии файла до удаления метаданных невозможно. Однако, если файл был каким-то образом скопирован или сохранён до удаления метаданных, то информация в этих копиях может оставаться доступной.

Тщательное удаление метаданных повышает конфиденциальность, но всегда стоит помнить о возможности наличия копий файлов до удаления метаданных. Если конфиденциальность является критически важной, рекомендуется использовать надежные инструменты и регулярно проверять файлы на наличие метаданных.

Начало формы

1. **Соблюдение принципов минимальных прав доступа**: Давайте доступ к конфиденциальной информации только тем, кто действительно его нуждается, и только к той информации, которая им необходима.

Принцип наименьших привилегий помогает ограничить возможный ущерб от следующих сценариев:

*Взлом учётной записи:* Если учетная запись пользователя или приложения скомпрометирована, злоумышленник не сможет использовать высокие привилегии этой учетной записи для доступа к чувствительным данным или системным функциям.

*Ошибки**пользователя:* С ограниченными правами пользователи менее вероятно совершат действия, которые могут нанести вред системам или данным.

*Вредоносное ПО:* Если вредоносное ПО запустится в контексте учетной записи с минимальными правами, его возможности по нанесению ущерба будут значительно ограничены.

***Как соблюдать принцип минимальных прав доступа?***

*Анализ и планирование:* Оцените, какие именно права доступа необходимы каждому пользователю, приложению или системному процессу для выполнения их функций. Не предоставляйте более того, что действительно нужно.

*Регулярный пересмотр прав доступа:* Периодически пересматривайте и корректируйте права доступа для учетных записей на основе изменений в их роли или обязанностях.

*Использование ролевого доступа:* Применяйте ролевую модель доступа, где права доступа назначаются группам или ролям, а не индивидуальным пользователям. Это упрощает управление привилегиями и помогает в их стандартизации.

*Изоляция привилегированных процессов:* Используйте специализированные учетные записи для административных или критически важных функций. Обычным пользователям не следует иметь доступ к этим учетным записям для повседневной работы.

*Аудит и мониторинг:* Регулярно проводите аудит прав доступа и мониторинг использования привилегий. Это поможет выявлять несанкционированное использование привилегий или ошибки в настройках безопасности.

*Обучение и осведомленность:* Обучайте пользователей важности безопасности и последствиях неправильного использования прав доступа. Повышение осведомленности помогает предотвратить ошибки и усилить общую безопасность.

1. **Опасность использования социальных сетей**: Будьте осторожны с тем, что вы публикуете в социальных сетях. Хакеры могут использовать собранную информацию для различных целей, от кражи идентичности до фишинговых атак и социальной инженерии.

***Как злоумышленники используют информацию из соцсетей:***

*Сбор информации для кражи идентичности:* Злоумышленники могут собирать персональные данные, такие как полное имя, дату рождения, адрес, информацию о родственниках и друзьях, чтобы создать убедительный фальшивый профиль или даже для получения доступа к банковским счетам.

*Фишинг:* Используя собранную информацию, преступники могут отправлять целевые фишинговые письма, которые кажутся легитимными, потому что содержат личную информацию и кажутся более убедительными.

*Социальная инженерия:* Информация о недавних личных событиях (например, о поездках или важных жизненных изменениях) может быть использована для манипуляций и обмана вас или ваших знакомых.

*Распространение вредоносного ПО:* Злоумышленники могут отправлять ссылки на вредоносное ПО через личные сообщения или комментарии, особенно если они создают фальшивые аккаунты друзей или знакомых.

***Как обезопасить себя:***

*Приватность профиля:* Настройте конфиденциальность вашего профиля в социальных сетях так, чтобы ваша личная информация была доступна только друзьям или определенным группам людей. Регулярно проверяйте настройки приватности, так как политики платформ могут меняться.

*Осторожность с личной информацией:* Избегайте публикации чувствительной информации, такой как адрес дома, номер телефона, данные паспорта или финансовой информации.

*Осмотрительность при принятии запросов в друзья***:** Принимайте запросы в друзья только от тех, кого вы лично знаете, и проверяйте профили на подлинность, прежде чем добавлять их.

1. **Безопасное удаление информации**: Когда информация больше не нужна, убедитесь, что она была безопасно удалена и не может быть восстановлена.

Чтобы удалить информацию с вашего устройства так, чтобы её нельзя было восстановить, вам нужно использовать методы, которые не просто удаляют данные, а перезаписывают их на физическом носителе. Это обеспечивает их полное стирание.

***Использование специализированного программного обеспечения***

*Для жёстких дисков и флеш-накопителей:* Используйте программы, такие как DBAN (Darik's Boot and Nuke), Eraser или CCleaner. Эти инструменты предлагают возможность безвозвратного удаления данных, перезаписывая их несколько раз.

*Для смартфонов и планшетов:* Используйте функцию "сброс до заводских настроек" (factory reset). Для большей надёжности используйте программы, предназначенные для перезаписи памяти устройства после сброса.

***Физическое уничтожение носителя***

*Физическое разрушение:* Если данные особенно чувствительные, физическое уничтожение диска может быть самым надёжным вариантом. Это может включать дробление, прожиг или демагнетизацию. Существуют специализированные службы, которые могут профессионально уничтожить физические носители информации.

***Перезапись данных***

Для того чтобы убедиться, что данные невозможно восстановить, некоторые программы предлагают перезаписать носитель данными (например, случайными числами) несколько раз. Это значительно усложняет любые попытки восстановления оригинальной информации.

***Шифрование данных перед удалением***

Если вы шифруете данные на диске до начала процесса удаления, то даже если данные будут каким-то образом восстановлены, без ключа шифрования они будут бесполезны. Это может быть особенно полезно, если вы не можете физически уничтожить носитель или использовать программное обеспечение для безвозвратного удаления.

***Профессиональные услуги***

Если вы не уверены в своих способностях безопасно уничтожить данные, можно обратиться к профессиональным сервисам, которые специализируются на уничтожении данных. Они используют сертифицированные методы для гарантии того, что данные не будут восстановлены.

***Важно:***

При использовании программного обеспечения для стирания данных убедитесь, что оно совместимо с вашим носителем (SSD, HDD, USB и т.д.), так как технологии накопителей различаются и требуют разных подходов к безопасному удалению данных.

1. **Использование средств для обнаружения несанкционированного доступа к устройствам и мониторинга сети**: Устанавливайте на своих устройствах средства для обнаружения несанкционированного доступа и мониторинга активности в сети.

Для обнаружения несанкционированного доступа к устройствам и мониторинга сети существует множество инструментов, которые помогают обнаруживать подозрительную активность, анализировать трафик сети и защищать устройства от вредоносных атак.

***Системы обнаружения и предотвращения вторжений (IDS/IPS)***

*Примеры:* Snort, Suricata.

*Как пользоваться:* Эти системы анализируют трафик сети на предмет подозрительных паттернов, которые могут указывать на попытку вторжения. Snort, например, можно настроить для мониторинга трафика на определённых портах и отправки уведомлений, если обнаруживаются аномалии. Suricata предлагает более продвинутые возможности анализа и может работать в многопоточном режиме для повышения производительности.

***Системы управления журналами и событиями безопасности (SIEM)***

*Примеры:* Splunk, SolarWinds, LogRhythm.

*Как пользоваться:* SIEM-системы собирают и агрегируют журналы с различных систем и устройств, анализируют их на предмет подозрительной активности. Например, Splunk позволяет создавать сложные запросы для анализа данных и настраивать панели управления для визуализации сетевой активности.

***Платформы мониторинга сети***

*Примеры:* Wireshark, PRTG Network Monitor, Zabbix.

*Как пользоваться:* Инструменты, такие как Wireshark, позволяют захватывать и анализировать пакеты данных в реальном времени. PRTG и Zabbix предоставляют комплексные решения для мониторинга сетевой инфраструктуры, обнаружения отказов устройств и оповещения администраторов о проблемах.

***Средства мониторинга доступа к файлам***

*Примеры:* Netwrix Auditor, ManageEngine FileAudit Plus.

*Как пользоваться:* Эти инструменты помогают отслеживать доступ к файлам и папкам на серверах и рабочих станциях, регистрируя, кто, когда и что делал с файлами. Настройка правил и уведомлений поможет быстро реагировать на несанкционированные или подозрительные действия.

***Инструменты защиты от вредоносного ПО***

*Примеры:* Malwarebytes, Kaspersky, Norton.

*Как пользоваться:* Антивирусные программы и решения для защиты от вредоносного ПО обеспечивают базовый уровень защиты, сканируя файлы и процессы на предмет известных угроз. Регулярное обновление баз данных вирусов и настройка реального времени сканирования повышают эффективность защиты.

1. **Защита идентичности**: Используйте псевдонимы и анонимные учетные записи при работе над чувствительными темами, чтобы защитить свою личную и профессиональную идентичность.

***Как использовать анонимные учетные записи:***

*Выбор псевдонима:* Создайте учётную запись, используя псевдоним, который не связан с вашим настоящим именем, адресом или другими личными данными.

*Использование временных email-адресов:* Для регистрации и подтверждения учетной записи используйте временный email-адрес или сервисы, предоставляющие анонимные почтовые ящики (например, ProtonMail, TempMail).

*Отказ от ввода личной информации:* Не вводите в профиль информацию, которая может раскрыть вашу личность, такую как место жительства, телефон или дата рождения.

*Использование VPN или Tor:* Чтобы скрыть ваш IP-адрес и местоположение, используйте VPN-сервисы или сеть Tor при регистрации и использовании анонимной учетной записи.

*Безопасные платформы:* Регистрируйтесь на платформах, которые уважают конфиденциальность пользователей и не требуют лишней личной информации.

*Избегание персонализированных настроек:* Не используйте персонализацию, которая может основываться на вашем поведении в сети или других данных, связанных с предыдущей активностью.

***Преимущества анонимных учетных записей:***

*Защита личной информации:* Минимизация риска утечек личной информации.

*Безопасность:* Защита от киберпреступников, которые могут использовать личную информацию для атак фишинга или мошенничества.

***Риски анонимных учетных записей:***

*Ограниченный доступ к некоторым функциям:* Некоторые сервисы могут ограничивать возможности, доступные анонимным пользователям.

*Сложности с восстановлением доступа:* Если вы забудете пароль, восстановить доступ к анонимной учетной записи может быть сложнее, так как вы не сможете использовать стандартные методы восстановления через личную почту или телефон.

1. **Контроль над физическим доступом к устройствам**: Убедитесь, что ваши устройства находятся в безопасности и не могут быть легко украдены или скомпрометированы. Используйте замки для ноутбуков и безопасные хранилища для хранения.

Защита ноутбука, телефона и планшета от кражи и утери требует комплексного подхода, включающего физические меры безопасности, использование программного обеспечения и предварительную подготовку для возможности восстановления данных или удаления их в случае кражи.

***Физические меры безопасности***

*Использование замков:* Для ноутбуков можно использовать кабельные замки, которые прикрепляются к специальному слоту на корпусе устройства и закрепляют его за неподвижный объект.

*Защитные чехлы:* Используйте защитные чехлы с замками для планшетов и телефонов, чтобы усложнить быстрый захват устройства.

*Безопасное хранение:* Не оставляйте устройства без присмотра в общественных местах. Используйте закрытые отсеки для хранения в автомобилях, а также сейфы в гостиницах. Будьте особенно внимательны в местах с большим скоплением людей, таких как аэропорты, кафе или общественный транспорт.

***Программное обеспечение и настройки***

На большинстве смартфонов, планшетов и некоторых ноутбуков есть функции поиска устройства, такие как «Найти мой iPhone» на iOS или «Найти устройство» на Android. Для Windows-ноутбуков можно использовать программы сторонних производителей.

***Системы сигнализации и трекинга***

*Приложения-трекеры:* Существуют приложения, которые отправляют уведомления при перемещении устройства без разблокировки. Эти приложения могут также активировать сигнал тревоги.

*Метки Bluetooth:* Используйте Bluetooth-трекеры, которые можно прикрепить к устройству и отслеживать через специальное приложение на смартфоне.

Международный фонд защиты свободы слова "Әділ сөз"

+7 777 400 22 10

info@adilsoz.kz

050000, г. Алматы, ул. Кунаева, 21Б, офис 41

Мы в соцсетях: