Перевертун Д.Р. Защита мобильных устройств: секреты безопасности смартфонов и планшетов // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 10(36) с. 67–70

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ: СЕКРЕТЫ БЕЗОПАСНОСТИ СМАРТФОНОВ И ПЛАНШЕТОВ

Перевертун Д.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com

Статья "Защита мобильных устройств: секреты безопасности смартфонов и планшетов" предоставляет подробное руководство по обеспечению безопасности мобильных устройств. В ней рассматриваются ключевые меры, которые пользователи могут принимать для защиты своих смартфонов и планшетов от различных киберугроз, включая установку паролей, использование биометрической аутентификации, обновление операционной системы и приложений, а также много других советов по обеспечению безопасности данных и личной информации.

Ключевые слова: Информационная безопасность, Мобильные устройства, Смартфоны, Планшеты, Пароль, Биометрическая аутентификация, Обновление операционной системы, Защита данных, Удаленное управление, Виртуальная частная сеть (VPN), Фишинг, Антивирусное программное обеспечение, Двухфакторная аутентификация, Облачное хранилище данных, Обучение по информационной безопасности, Резервное копирование данных, Операционные системы мобильных устройств, Wi-Fi безопасность, Удаление данных, Способы защиты мобильных устройств.

MOBILE DEVICE PROTECTION: SECRETS OF SMARTPHONE AND TABLET SECURITY

Perevertun D.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com

The article "Protection of mobile devices: Secrets of smartphone and tablet security" provides a detailed guide to ensuring the security of mobile devices. It discusses the key measures that users can take to protect their smartphones and tablets from various cyber threats, including setting passwords, using biometric authentication, updating the operating system and applications, as well as many other tips for ensuring the security of data and personal information.

Keywords: Information security, Mobile devices, Smartphones, Tablets, Password, Biometric authentication, Operating System update, Data protection, Remote management, Virtual Private Network (VPN), Phishing, Antivirus software, Two-factor authentication, Cloud data storage, Information security training, Data backup, Mobile operating systems devices, Wi-Fi security, Data deletion, Ways to protect mobile devices.

Мобильные устройства, такие как смартфоны и планшеты, стали неотъемлемой частью нашей повседневной жизни. Они хранят большое количество личной и чувствительной

информации, что делает их привлекательной целью для хакеров и киберпреступников. Поэтому обеспечение безопасности мобильных устройств становится критически важной задачей для всех пользователей. В этой статье мы рассмотрим некоторые основные секреты безопасности, которые помогут вам защитить ваш смартфон или планшет.

Первым и одним из самых важных шагов в обеспечении безопасности мобильного устройства является установка пароля или PIN-кода. Это защищает ваше устройство от несанкционированного доступа, даже если оно украдено или потеряно.

Используйте биометрическую аутентификацию. Многие современные смартфоны и планшеты оснащены биометрическими методами аутентификации, такими как сканер отпечатков пальцев или распознавание лица. Они предоставляют удобный и надежный способ разблокировки устройства.

Обновляйте операционную систему и приложения. Регулярные обновления операционной системы и приложений не только улучшают функциональность вашего устройства, но и закрывают уязвимости, которые могли бы использовать хакеры. Важно включать автоматическое обновление, чтобы всегда иметь последние версии.

Устанавливайте только надежные приложения. При установке приложений следует придерживаться официальных магазинов приложений, таких как Google Play Store или App Store. Это помогает избежать установки вредоносных программ.[1-2}

Включите удаленную блокировку и удаление данных. Многие устройства предоставляют возможность удаленно блокировать и стирать данные с утерянных или украденных устройств. Активируйте эту функцию и настройте удаленный доступ к ней, чтобы быть готовыми к любым непредвиденным ситуациям.

Используйте виртуальную частную сеть (VPN). VPN обеспечивает шифрование интернет-соединения, защищая ваши данные от кибершпионов и злоумышленников. Это особенно важно при подключении к общественным Wi-Fi сетям.

Остерегайтесь фишинга и мошенничества. Будьте осторожными при нажатии на ссылки в текстовых сообщениях или электронной почте. Фишеры используют различные методы обмана для получения вашей личной информации.

Шифруйте важные данные. Если у вас на устройстве хранятся особо чувствительные данные, используйте приложения для шифрования, чтобы защитить их от несанкционированного доступа.

Соблюдение этих секретов безопасности поможет вам укрепить защиту вашего мобильного устройства и защитить ваши личные данные от потенциальных угроз. В мире, где информационная безопасность играет все более важную роль, забота о безопасности вашего смартфона или планшета - это залог защиты вашей частной жизни и данных.

Включите двухфакторную аутентификацию. Двухфакторная аутентификация (2FA) добавляет дополнительный слой безопасности к вашему устройству. После ввода пароля или PIN-кода, вам может потребоваться предоставить дополнительный код, который обычно отправляется на ваше доверенное устройство. Это усложняет задачу злоумышленникам, пытающимся получить доступ к вашей учетной записи.

Регулярно создавайте резервные копии данных. Иногда безопасность не может быть гарантирована, и ваше устройство может быть повреждено, утеряно или заражено

вредоносным программным обеспечением. Регулярное создание резервных копий данных поможет вам восстановить важную информацию в случае чего-либо непредвиденного.

Ограничьте доступ к приложениям и данным. Настройте разрешения приложений так, чтобы они имели доступ только к необходимым данным и функциям. Это уменьшит риск утечки информации.

Обучение сотрудников. Если у вас есть корпоративные мобильные устройства, обучите сотрудников базовым принципам безопасности, чтобы предотвратить потенциальные угрозы для бизнеса.

Удаляйте неиспользуемые приложения и данные. Неиспользуемые приложения и данные могут быть уязвимыми точками в системе. Регулярно удаляйте приложения и файлы, которые вам больше не нужны.

Следите за новостями о безопасности. Оставайтесь в курсе последних событий и угроз в мире информационной безопасности. Это поможет вам адаптировать свои методы защиты к современным угрозам.

Убедитесь, что ваше устройство подключено только к надежным и защищенным Wi-Fi сетям. Публичные Wi-Fi сети могут быть уязвимыми для атак, поэтому избегайте отправки чувствительных данных, если не уверены в безопасности сети.[3-4]

Используйте специализированные мобильные антивирусные программы. На рынке существует множество приложений для мобильных устройств, предназначенных для обнаружения и удаления вредоносного программного обеспечения. Установите надежное антивирусное приложение и регулярно сканируйте устройство.

Постоянно проверяйте свои финансовые операции. Если вы используете мобильное приложение для банковских операций, регулярно проверяйте свои транзакции на предмет подозрительных действий. Своевременное обнаружение аномалий может помочь предотвратить финансовые убытки.

Осознайте риски использования облачных служб. Пользуйтесь облачными хранилищами с осторожностью и убедитесь, что ваши данные надежно зашифрованы. Используйте сильные пароли и двухфакторную аутентификацию для доступа к облачным аккаунтам.

Рассмотрите возможность удаления чувствительных данных. Если у вас нет необходимости хранить определенные чувствительные данные (например, старые сообщения, фотографии или файлы), рассмотрите возможность их удаления. Это уменьшит вероятность утечки данных при возможных инцидентах.

Обучение и осведомленность. Обучение и осведомленность - это ключевые аспекты информационной безопасности. Постоянно обновляйте свои знания о современных угрозах и методах защиты. Обучайте семью и близких к базовым принципам безопасности.

Защита мобильных устройств - это долгосрочный процесс, и она требует внимания и осторожности. [5] Соблюдение этих советов и секретов безопасности поможет вам сохранить вашу ценную информацию в безопасности и спокойно пользоваться вашими мобильными устройствами. Не забывайте, что инвестирование времени и усилий в обеспечение безопасности сегодня может сэкономить вам немало проблем в будущем.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.
2. Гельфанд А. М. и др. Интернет вещей (IoT): Угрозы безопасности и конфиденциальности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике//Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С.И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N.A., Timofeev R.S. Comparison of training methods for convolutional neural networks//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
6. KOSOV N.A., MAZEPIN P.S., GRISHIN N.A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.