Секция социальных педагогов

«Как помочь ребенку избежать опасности, подстерегающие в сети Интернет»

Н.Н.Дорофеева, руководитель МО социальных педагогов Курчатовского района

Цель: повышение уровня информационной компетентности социальных педагогов по вопросу хранения персональных данных в смартфоне или другом «умном» устройстве с целью безопасного использования мобильного устройства и хранения персональных данных.

Задачи:

1) сформировать понятийный аппарат по вопросам защиты персональных данных;
2) сформировать представление об основных механизмах защиты своих персональных данных в мобильном устройстве;
3) формирование у педагогов навыков безопасного использования мобильного устройства и основ безопасного использования персональных данных.

Форма: практическое занятие.

Формы и методы занятия:

- беседа
- игра

Планируемые результаты:

- научиться использовать основные механизмы защиты своих персональных данных;
- приобрести навыки трансляции полученных компетенций для участников образовательных отношений, используя различные формы и методы обучения.

Введение в тему:

Цель: знакомство с вариантами распространения персональных данных через мобильные приложения.

Разминка «Никто, кроме моего смартфона, не знает, что я...»

Задача: помочь учащимся осознать, какие персональные данные хранятся на их смартфоне.

Необходимые материалы: небольшой мячик.

Время проведения: 5 минут.

Процедура проведения

«У каждого из нас есть мобильный телефон или смартфон, в котором хранится много важной и полезной информации, в том числе и наши персональные данные. Записная книга хранит контакты, мессенджеры — переписку с друзьями, игровые приложения — историю наших побед и поражений и т.д. Иногда создается впечатление, что наш телефон знает о нас гораздо больше, чем наши родственники и друзья».

Ведущий предлагает учащимся сыграть в следующую игру.

Ведущий берет мяч в руки и говорит фразу, начинающуюся со слов *«Никто, кроме моего смартфона, не знает, что я...»* (возможные варианты ответов: *выиграл в онлайн-шахматы90 партий из 100, переписываюсь с другом из Люксембурга,пробежал в прошлое воскресенье 25 км и т.д.*). Затем ведущий бросает мяч любому участнику группы. Задача участника — придумать свое окончание фразы *«Никто, кроме моего смартфона, не знает, что я...»* и передать мяч следующему игроку.

Игра продолжается до тех пор, пока все учащиеся не скажут свой вариант ответа.

Обсуждение

Легким или сложным показалось вам это упражнение? Почему?

Какой из вариантов фразы показался самым необычным или запомнился больше всего? Почему?

Как по-вашему, то, что наши смартфоны так много знают о нас — хорошо или плохо? Почему?

Основная часть

В соответствии со статьей 7 Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ лица (далее-Закон), получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных. В настоящее время все чаще номера телефонов передаются и используются без согласия абонента, так как в законодательстве четко не указано, что они являются персональными данными.

Казалось бы, набор цифр номера телефона никак не может персонифицировать субъекта персональных данных, он полностью обезличен. Но добавьте к этим цифрам ФИО, и ситуация в корне изменится. Плюс, если этот номер закреплен за конкретным физическим лицом по договору с оператором связи, то говорить об обезличенности набора цифр вовсе не приходится.

И действительно, согласно ст. 3 Закона, персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных), то есть его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, в связи с чем можно сделать вывод, что номер мобильного телефона также является персональными данными.

Но ст. 3 Закона также вводит понятие обезличивания персональных данных, которое включает в себя действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. Сам по себе номер телефона без указания сведений о его владельце, является информацией обезличенной, то есть набор цифр нельзя признать персональной информацией.

А вот если номер телефона использован с указанием на ФИО его владельца, то такая информация уже носит характер конфиденциальной, и может быть использована только с согласия субъекта персональных данных на обработку его персональных данных.

Ст. 44.1. Закона «О связи» 07.07.2003 N 126-ФЗ с изменениями, вступившими в силу 21.10.2014г., также закрепляет, что если по номеру телефона можно как-либо идентифицировать абонента, то необходимо согласие абонента, например, на рассылку рекламной информации.

Выводы:

1. Номер телефона является персональными данными;
2. Передача персональных данных третьим лицам без согласия субъекта персональных данных незаконна;
3. Использование номеров телефонов в случае отсутствия дополнительных сведений об их владельцах также требует согласия**.**

Какие ПД хранит само мобильное устройство?

Что нужно сделать чтобы защитить ПД, которые находятся в телефоне?

Обновление ОС и используемых приложений

Включите автоматическое обновление приложений на вашем телефоне или попросите систему уведомлять вас о наличии новинок, чтобы не упустить момент. И всегда загружайте обновления операционной системы, как только вам будет предложено это сделать.

Зачем это нужно? Чтоб предотвратить взлом телефона через уязвимости в ОС и приложениях. Когда авторы программ и игр обновляют свой софт до более новых версий, они составляют отчет об исправленных ошибках. Результаты исправлений они выкладывают на всеобщее обозрение, поэтому хакеры берут эти данные и направляют свои атаки на тех пользователей, которые ОС либо приложение не обновили и оставили свои смартфоны или аккаунты в соцсетях уязвимыми.

Загрузка только из проверенных источников

1. При загрузке приложений пользуйтесь только проверенными магазинами вроде AppStore и GooglePlay – это официальные источники, где приложения проверяют перед выставлением на всеобщее обозрение и скачиванием обычных пользователей. Поэтому там гораздо меньше шансов нарваться на вредоносное ПО. Когда же программа скачана с неофициального магазина или сайта, где размещают нелицензионные материалы, то последствием может стать взлом телефона.
2. Подозрительные приложения могут иногда попадаться даже в официальных магазинах. Чтоб избежать обмана, внимательно изучайте информацию о приложении, смотрите на отзывы пользователей, количество скачиваний и общий рейтинг программы.
3. Следите за разрешениями, которые у вас просят приложения при установке или запуске. Это может быть доступ к личным фото, смс-переписке, совершению звонков и особым функциям, например, к функциям разработчика. Всего одно неверное решение – и мошенники смогут получить удаленный доступ к вашему смартфону.

Отказ от получения Root-прав

В Интернете вы могли встречать обсуждения преимуществ, которые дает установка специальных приложений, дающих пользователю ОС AndroidRoot-права. Это означает, что с их помощью можно полностью редактировать «внутренности» смартфона, удалять приложения, которые обычно нельзя удалить, например, стандартные, получить доступ к системным папкам и файлам, улучшить производительность устройства.

Однако вместе с неограниченными возможностями вы делаете свой смартфон уязвимым к хакерским атакам. В случае, когда такие права получит вредоносное приложение, оно будет иметь доступ ко всем файлам на вашем мобильном устройстве, даже к таким, как чтение смс для восстановления доступа к аккаунту и подтверждение банковских операций.

Осторожность в использовании публичного Wi-Fi

Когда вы однажды подключитесь к какой-либо беспроводной сети, ваш смартфон запомнит пароль и при нахождении этой сети во второй раз подключится к ней автоматически. Если сеть не защищена паролем, то и запоминать ничего не придется. Казалось бы, очень удобно, но есть один момент. Мошенники могут создавать свои горячие точки вместо знакомых вам точек с Wi-Fi, и называть их тем же именем. Если вы подключитесь к такой точке, то злоумышленник получит доступ ко всем передаваемым данным и будет следить за вашими действиями в сети, а позже по собранным сведениям сможет осуществить взлом телефона.

Чтобы такого не произошло, советуется не подключаться к публичным беспроводным сетям, не защищенным паролем, а также очищать список всех сетей, которые «запомнил» ваш телефон. Не ленитесь записать пароли к используемым вами точкам и вводите его каждый раз при подключении, чтобы защитить смартфон от взлома.

- Когда же есть необходимость использовать публичные Wi-Fi сети, пользуйтесь VPN-сервисами, которые шифруют ваше Интернет-соединение и защищают ваши данные, чтоб их нельзя было перехватить и осуществить взлом.

Отключение сетей Wi-Fi и Bluetooth

Снизить риск взлома телефона поможет отключение сетей Wi-Fi и Bluetooth, когда вы ими не пользуетесь. Тогда у хакера не будет возможности осуществить удаленный доступ к вашему мобильному устройству. С одной стороны, злоумышленник может дождаться момента, когда вы вновь подключитесь к одной из сетей, но с другой – не сумев взломать ваш телефон, он может бросить эту затею, если его цель – массовый взлом аккаунтов, а не именно вы.

Контроль SMS-переписок

Игнорирование подозрительных ссылок, смс-сообщений – тоже хорошая защита от взлома. Многие хакерские атаки и распространение вирусов начиналось именно переходом невнимательных пользователей по вредоносным ссылкам. Но осторожным

нужно быть, не только открывая ссылки в Интернете, а и получая SMS. Обращайте внимание на подозрительные сообщения со странными запросами, даже когда они пришли от вашего друга – его смартфон тоже могли взломать.

Использование сложного пароля

Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но чтобы взломать семисимвольный пароль, потребуется два-четыре года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

Итог занятия

Смартфоны и другие «умные» устройства все активнее проникают в нашу жизнь, делая ее более комфортной и удобной. Однако за это удобство нам приходится платить — нашимиперсональными данными. Без преувеличения можно сказать, чтонаши смартфоны порой знают о нас больше нас самих. Поэтомумы должны с осторожностью использовать смартфоны и другиегаджеты, защищать их антивирусными программами и надежными паролями. Устанавливая новые приложения на смартфон, следует внимательно ознакомиться с условиями, предлагаемымиразработчиками.