Доклад

Защита персональных данных в социальных сетях

Неустроева Ирина Николаевна

Содержание

Список иллюстраций

Список таблиц

1 Актуальность

Стремительное развитие цифровых технологий, увеличением пользователей сети Интернет создало новую виртуальную платформу для совершения неправомерных деяний для злоумышленников. Число утечек персональных данных как во всем мире, так и в России неутомимо возрастает. Много людей подвергаются проблеме утечки личных данных из-за невнимательности или неопытности

2 Цели и задачи

1. Определить, что такое персональные данные.
2. Выделить основные типы персональных данных в социальных сетях.
3. Выявить способы защиты личных данных.
4. Определить дальнейшие действия, если персональные данные были украдены

3 Объект и предмет исследования

Социальные сети, и правило безопасности при их использовании

4 Основная часть

4.1 Персональные данные

Персональные данные – это любая информация, относящаяся к прямо или косвенно определенному физическому лицу (субъекту персональных данных).

Другими словами, персональные данные — это информация, по которой можно идентифицировать человека. Например, к ней относится имя и фамилия, дата рождения, адрес проживания, логины и пароли от различных сервисов.

4.2 Чем опасна потеря персональных данных ?

Личные данные могут быть использованы третьими лицами для навязывания рекламных услуг, шантажа, регистрации на сомнительных платформах, кражи логинов и паролей от банковских приложений, выманивания денег посредством фишинга.

4.3 Виды персональных данных в соцсетях

1. Регистрационные: Их мы раскрываем, когда создаём аккаунт: имя, фамилия, пол, возраст, место жительства, номер телефона, email, профессия, семейное положение, интересы, смена работы, города, семейного статуса.

2. Биометрические персональные данные: Представляют собой сведения о

наших биологических особенностях. К таким данным относятся: отпечаток пальца, рисунок радужной оболочки глаза, слепок голоса и пр.

3. Фотографии и видео: Визуальный контент, размещенный в социальных сетях

4. Логины и пароли: Учетные данные пользователя, используемые для доступа в социальные сети

5. Специальные персональные данные: К ним относиться, расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья и пр.

6. Цифровые персональные данные: Номер и серия паспорта, СНИЛС, ИНН, номер банковского счета, номер банковской карты.

7. Геоданные: Местоположение и перемещения пользователя

4.4 Способы защиты персональных данных

1. Надежный пароль - Это первый инструмент базовой защиты

Пароль должен соответствовать требованиям:

1) Уникальный , для каждого сервиса пароль должен быть разный

2) Представлять из себя набор случайных символов, а сами символы самые разные — «»:jhhK0%№_(1»

3) Состоять как минимум из 12 символов

4) Не содержать личной информации о пользователе

5) Обновляться каждые пол года

2. Двухфакторная аутентификация

чтобы максимально обезопасить от взлома свой аккаунт, используйте двухфакторную аутентификацию

На первом этапе обычно вводится пароль. А для второго этапа используют разные способы подтверждения:

- Код в SMS, который придет на телефон, указанный при регистрации пользователя.
- Код из письма на email, указанный при регистрации.
- Специальные приложения, например, Яндекс Ключ или Google Authenticator. В них можно получать коды для входа в аккаунт, даже если нет подключения к интернету.
- Резервные коды. Их генерируют заранее, а затем вводят, если нет возможности получить код по SMS или на email.
- Биометрия, например, отпечатки пальцев или селфи.

3. Цифровая гигиена

- Не делитесь слишком личной информацией в социальных сетях и будьте внимательны при публикации контента в интернете
- Отключите геолокацию в приложениях, где это не мешает работе программы
- Не выкладывайте свои документы в социальные сети

4. Очищайте Cookies

Cookies- Это фрагмент данных о сайтах, на которые вы раньше заходили, запоминающий историю покупок, наполнение корзины, сведения о вашей активности и интересах

Фалы Cookie могут быть использованы, как и для сбора необходимых данных, так и для целевой рекламы

Очищайте куки в настройках браузера время от времени

5. Используете защищенное интернет соединение

- Избегайте использование общественных Wi-Fi сетей
- Публичные сети Wi-Fi обычно не шифруют трафик, кто угодно может подсмотреть, что вы отправляете и получаете, подключившись к той же точке доступа.
- Старайтесь не передавать таким образом логины, пароли, данные кредитных карт и тому подобное. Лучше всего использовать VPN, чтобы зашифровать передачу данных и защитить их от посторонних глаз.
- Отдавайте предпочтение сайтам HTTPS. Зашифрованное соединение HTTPS защищает передаваемые данные от перехвата. Чтобы убедиться, что сайт, на который вы заходите, использует этот протокол, в адресной строке должно быть “https://”

6. Условия использования приложением

1) Изучите политику конфиденциальности

Приложения запрашивают доступ к учётной записи в соцсети, камере, местоположению, контактам, но далеко не все дают гарантию безопасности. Доверять нужно только проверенным сервисам.

2) Регулярно обновляйте приложение

В каждом приложении есть уязвимости — лазейки, через которые хакер может получить доступ к данным. Чтобы обезопасить пользователей, разработчики находят уязвимости, устраняют их и выпускают новую версию приложения.

3) Не привязывайте банковские карты к профилю

Во многих социальных сетях есть возможность привязать к аккаунту банковскую карту для внутренних платежей. Но так платёжные данные подвергаются дополнительной опасности, как только аккаунт будет взломан

- Рекомендую для платежей в соцсетях завести отдельную карту — можно виртуальную

4.5 Дальнейшие действия, если персональные данные были украдены

1. Завершите сессии и смените пароль
2. Если к учётной записи привязаны банковские карт, лучше заблокировать их до возвращения доступа
3. Предупредите близких и друзей о том, что аккаунт взломали. Важно действовать быстро — пока люди не перевели мошенникам деньги
4. Если доступ к профилю закрыт, попробуйте восстановить пароль через телефон или почту
5. Попросите друзей пожаловаться на вашу взломанную страницу. Чем больше жалоб, тем быстрее мошенника заблокируют

5 Вывод

В ходе работы, выяснили, что необходимо внимательно относиться к созданию и хранению паролей, использовать защищенное интернет соединение, помнить о цифровой гигиене, Очищайте Cookies, чтобы защитить свои персональные данные в социальных сетях.

5.1 Список литературы

1. Использование и защита персональных данных в социальных сетях Интернета» — научная статья П. Б. Филиппова, «Прикладная информатика» 2012 г

2. Защита персональных данных в социальных сетях, Чернобаев С.В. Российский экономический университет имени Г.В. Плеханова (117997, г. Москва)

3. Мамедов Р. Защита персональных данных в социальных сетях. http://www.itsec.ru/articles personalnyh-dannyh-v-sotsialnyh-setyah

4. Халилов Д. Способы защиты персональных данных в социальных сетях/ URL: http://www.praima.ru/node/351

1 ::: {#refs} :::