Центр мониторинга социальных сетей
ГБУ ДПО ЧИРПО

ул. Воровского, д.36, г. Челябинск, 454092
Тел.: +7 (351) 222 07 56 (доп. 126)
Kiber-lab@ya.ru

КОНСПЕКТ КЛАССНОГО ЧАСА ПО ТЕМЕ: «ПРОФИЛАКТИКА СЛУЧАЕВ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ»

В настоящее время с учетом цифровизации и виртуализации нашей повседневной жизни – важной темой для обсуждения становятся вопросы, связанные с практиками медиабезопасности.

Вопросы обучающимся. *Каковы, на ваш взгляд, самые актуальные угрозы, с которыми мы можем столкнуться в сети интернет?*

В широком смысле *медиабезопасность* – обеспечение государством информационной безопасности граждан, защита физического, умственного и нравственного развития, а также человеческого достоинства во всех аудиовизуальных медиа-услугах и электронных СМИ. Очень часто понятие медиабезопасности современные исследователи и педагоги связывают только с молодежью, детьми и подростками, хотя на самом деле эта проблема касается всего общества в целом, поскольку, прежде всего, медиабезопасность каждого человека зависит от его собственных умений «фильтровать» предложенную информацию.

Говоря про вопросы медиабезопасности, важно понимать и определение понятий «медиа-угрозы» или «информационные угрозы». *Медиа-угрозы* (информационные угрозы) – потенциально возможные события, процессы или явления, которые посредством воздействия на информацию или другие компоненты информационной системы могут прямо или косвенно привести к нанесению ущерба интересам различных субъектов.

В настоящее время исследователи проблем медиабезопасности выделяют следующие потенциальные источники медиа-угроз:

- ✓ существенное расширение возможности манипулирования сознанием человека за счет формирования вокруг него индивидуального «виртуального информационного пространства»;
- ✓ возможность использовать технологии воздействия на психическую деятельность человека;
- ✓ сбор и использование в корыстных целях персональных данных пользователя интернет-пространства;
- ✓ манипуляция общественным мнением относительно отношения к тем или иным общественным событиям.

Данные медиа-угрозы могут быть потенциально реализованы в следующих проблемных формах:

- ✓ *контентные* – материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, нецензурную лексику и т.д.;

✓ *коммуникационные* (связаны с межличностными отношениями интернет-пользователей), например, незаконный контакт, домогательство, киберпреследование, кибербуллинг (травля, оскорбления или угрозы, высказываемые жертве с помощью средств электронной коммуникации, в частности, сообщений в социальных сетях, мгновенных сообщений, электронных писем и СМС);

✓ *электронные* – возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д.;

✓ *потребительские* – злоупотребление в интернете правами потребителя.

При этом для выстраивания стратегий собственной безопасности необходимо знать ключевые правила безопасности данной сферы.

Вопросы обучающимся. *Все мы активно пользуемся социальными сетями. Скажите, вы зарегистрированы в социальной сети? В какой? А знаете ключевые правила безопасного поведения в социальных сетях?*

Основные советы по безопасности в социальных сетях:

1. Ограничить список друзей. У вас в друзьях не должно быть случайных и незнакомых людей.

2. Защищать свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как вы и ваши родители планируете провести каникулы.

3. Защищать свою репутацию - задавайте себе вопрос: хотели бы вы, чтобы другие пользователи видели, что вы загружаете? Подумайте, прежде чем что-то опубликовать, написать и загрузить.

4. Если вы говорите с людьми, которых не знаете, не используйте свое реальное имя и другую личную информацию: имя, место жительства, место учебы и прочее.

5. Избегайте размещения фотографий в интернете, где вы изображены на местности, по которой можно определить ваше местоположение.

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если вас взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Вопросы обучающимся. *Пользуетесь ли вы электронной почтой? Знаете, какие правила безопасности при регистрации электронного адреса важно соблюдать?*

Электронная почта

Электронная почта – это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также, кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге.

2. Не указывайте в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13».

3. Используйте двухэтапную авторизацию (это когда помимо пароля нужно вводить код, присылаемый по SMS).

4. Выберите сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.

5. Если есть возможность придумать самому свой личный вопрос, используйте эту возможность.

6. Используйте несколько почтовых ящиков. Отдельный необходимо иметь для частной переписки с адресатами, которым вы доверяете - этот электронный адрес не надо использовать при регистрации на форумах и сайтах.

7. Не открывайте файлы и другие вложения в письмах даже если они пришли от ваших друзей. Лучше уточните у них, отправляли ли они вам эти файлы.

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

Вопросы обучающимся. *А какой у вас телефон? Кнопочный или обычный? Знаете ли ключевые правила безопасного использования смартфоном?*

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

1. Будьте осторожны, ведь когда вам предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.

2. Думайте, прежде чем отправить SMS, фото или видео. Вы точно знаете, где они будут в конечном итоге?

3. Необходимо обновлять операционную систему твоего смартфона.

4. Используйте антивирусные программы для мобильных телефонов.

5. Не загружайте приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.

6. После того как вы выйдете с сайта, где вводили личную информацию, зайдите в настройки браузера и удалите «cookies».

7. Периодически проверяйте, какие платные услуги активированы на вашем номере.

8. Давайте свой номер мобильного телефона только людям, которых вы знаете и кому доверяете.

9. Bluetooth должен быть выключен, когда вы им не пользуетесь. Не забывайте иногда проверять это.

Вопросы обучающимся*. А знаете, что такое персональные данные? Почему их не следует разглашать?*

Незаконное распространение, в том числе хищение личных данных

Главная цель фишинга (вида интернет-мошенничества) состоит в получении конфиденциальных данных пользователей – логинов и паролей. На английском языке phishing читается как фишинг (от «fishing» – рыбная ловля, «password» – пароль).

Основные советы по борьбе с фишингом:

1. Следите за своим аккаунтом. Если вы подозреваете, что ваша анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее.

2. Используйте безопасные веб-сайты, в том числе для посещения интернет-магазинов и поисковых систем.

3. Используйте сложные и разные пароли. Таким образом, если вас взломают, то злоумышленники получат доступ только к одному профилю в сети, а не ко всем.

4. Если вас взломали, то необходимо предупредить всех своих знакомых, которые добавлены в друзьях, о том, что вас взломали и, возможно, от вашего имени будет рассылаться спам и ссылки на фишинговые сайты.

5. Установите надежный пароль (PIN) на мобильный телефон.

6. Отключите сохранение пароля в браузере.

7. Не открывайте файлы и другие вложения в письмах, даже если они пришли от ваших друзей. Лучше уточните у них, отправляли ли они вам эти файлы.

Таким образом, соблюдая указанные выше правила, можно обезопасить себя от противоправных посягательств при нахождении в интернет-пространстве в рамках его использования.

Если Вы стали жертвой преступления, в обязательном порядке необходимо обратиться в полицию по телефону 112 или 02.

Берегите себя и своих близких!