СОВЕТЫ ПО ЗАЩИТЕ СЕБЯ ПРИ ПОКУПКАХ ЧЕРЕЗ ИНТЕРНЕТ

- Используй авторитетные и устоявшиеся в интернете сайты
- Перед заказом, необходимо точно знать цену, условия приобретения чего-либо, условия доставки и гарантийные условия. Если это не указано в анкете, то лучше всего будет лично связаться с продавцом и задать ему вопросы.
- Читай на сайте интернет-магазина соглашение о конфиденциальности.
- Убедись в возможности подать жалобу или/и отменить заказ.
- Когда вводишь свои личные данные желательно, чтобы в адресной строке браузера появился значок ключа. Это означает, что соединение безопасно и твои данные не будут украдены.
- На сайте магазина должен быть адрес, номер телефона или электронная почта для связи в случае возникновения вопросов.
- Узнай мнения других покупателей о том товаре, который ты хочешь приобрести. Таким образом, ты будешь гарантирован, что этот сайт не является копией какого-то сайта.
- Попытайся найти сертификаты сторонних организаций. Компании могут размещать эти сертификаты, если они соблюдают ряд жестких стандартов, которые определяют методы их работы.

Первая школа

МБОУ Обливская СОШ №1
E-mail учреждения: oblivsk@gmail.com
Телефон муниципального учреждении:
8 (863 96) 2-21-98
Адрес муниципального учреждения: 347140, Ростовская область, Обливский район, ст. Обливская, ул. Коммунистическая, 4

Заместитель директора, учитель информатики Ващинников Д.О.

Первая школа

Безопасность в сети Интернет

Ссылки на полезные ресурсы

http://сетевичок.рф/
http://i-deti.org/
https://www.google.ru/safetycenter/
http://informatics.ru/

Правила в сети интернет

СОВЕТЫ ПО ЗАЩИТЕ МОБИЛЬНОГО ТЕЛЕФОНА

- Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.
- Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
- Не принимай предложения, которые звучат слишком хорошо, чтобы быть правдой. Возможно это обман.
- Подумай, прежде чем нажимать на кнопку «Загрузить». Не открывай MMS и вложения в сообщениях электронной почты и SMS. Они могут содержать вредоносное программное ПО и перевести тебя на вредоносный веб-сайт.
- Обновляй операционную систему смартфона.
- Используй антивирус на смартфоне
- Не загружай приложения от неизвестного источника.
- После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.

- Не храни на смартфоне личную информацию, переноси ее на ПК.
- Периодически проверяй у оператора связи какие платные услуги активированы на твоем номере.
- Перед поездкой на отдых отключай приложения (игры, погода), которые делают запросы через интернет.

ФИШИНГ ИЛИ КРАЖА ЛИЧНЫХ ДАННЫХ

- Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее.
- Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем. Например, популярные сайты ты можешь добавить в закладки, и заходить на них через закладки.
- Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем. Также желательно использовать русские слова, набираемые в английской раскладке.
- Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты.
- Установи надежный пароль (PIN) на мобильный телефон. Таким образом если у тебя украдут телефон, то злоумышленники не получат твою личную информацию. Пароли в телефоне не храни.
- Отключи сохранение пароля в браузере.
- Не переходи по ссылкам в сообщениях электронной почты и сообщениях из социальной сети.

Не размещай личную информацию в интернете. Даже маленькие кусочки личных данных могут быть использованы в преступных целях.

МЕТОДЫ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

- Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
- Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
- Ограничь физический доступ к компьютеру для посторонних лиц;
- Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проференных источников;

Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Первая школа

МБОУ Обливская СОШ №1

Заместитель директора, учитель информатики Ващинников Д.О.