**Вопросы**

1. На ваш компьютер пришло сообщение странного содержания содержащее неизвестный вам файл .Что стоит делать при получении сообщения с неизвестным файлом(содержащим вирус)?

Варианты ответа:

отправить знакомому-программисту

удалить письмо из почты

не открывать

посмотреть что внутри

удалить свою почту и не пользоваться ей

создать приватный аккаунт и открыть письмо

не пересылать на другие адреса

ОТВЕТ:

1.Не открывать.  
2.Не пересылать на другие адреса.  
3.Удалить письмо из почты.

1. Вы сидите в вашем любимом парке и заметили общедоступный wifi. Решая подключится к такой сети каким рискам вы можете быть подвергнуты?

Варианты ответа:

Никаким

Мошенники могут найти мой дом

Мои данные будут украдены

Произойдет физическое нападение

Пароли, электронные письма будут украдены

Меня завербуют в армию

ОТВЕТ:

Общедоступный Wi-Fi может идентифицировать данные, которые передаются через сетевое устройство, такие как электронные письма, история просмотров, пароли и данные кредитных карт.

1. Отдыхая после трудного дня вы прочитали статью про “атаку грубой силой” в нем рассказывалось что это - метод проб и ошибок, чтобы узнать правильный пароль или PIN-код. Хакеры периодически пробуют все комбинации учетных данных. Как предотвратить атаку грубой силой?

Варианты ответа:

Убежать в другое место

Установка длины пароля

Создать новый аккаунт

Ничего

Увеличить сложность пароля

Установить лимит на ошибки входа

Написать другу-программисту

* ОТВЕТ: Установка длины пароля.
* Увеличьте сложность пароля.
* Установить лимит на ошибки входа.

1. Посетив интересное интервью от одного из работников сферы кибербезопасности вы решили что нужно немного обезопасить себя от кражи личных данных. Как можно реализовать эту идею?

Варианты ответа:

Создать уникальное имя пользователя и пароль

Использовать старые ненадежные сайты

Использовать антивирус

Создать собственные сайты

Удалить с устройств всё ненужное

Не передавать информацию через интернет

Использовать только надежные сайты

Верить людям из интернета

Сообщать всем свои данные

Использовать надежный веб-браузер

ОТВЕТ: Это можно предотвратить с помощью предоставления или использования уникального имени пользователя и пароля, не передавайте конфиденциальную информацию через Интернет. Только надежные или защищенные сайты должны быть использованы для бронирования и покупки. Всегда старайтесь использовать новейшие и безопасные веб-браузеры. Компьютеры или системы должны быть защищены антивирусными инструментами и периодически обновлять вашу систему и программное обеспечение.

1. Как можно обезопасить свои социальные сети и личные устройства от их взлома злоумышленниками, какие способы аутентификации нужно использовать?

Варианты ответа:

Использовать токен, пароль и биометрию

Использовать только токен

Использовать только пароль

Использовать только биометрию

Использовать токен и пароль

Использовать пароль и биометрию

Использовать токен и биометрию

ОТВЕТ: Аутентификация возможна при помощи следующих методов: что человек знает (пароль), что у человека есть (токен) и кто человек есть (биометрия).

**Стилистика**

* Под первый вопрос можно сделать на заднем фоне картинку почты и на ней неизвестный файл(желательно выделить). Можно сделать формат в виде викторины с ответами где нужно выделить правильные ответы (не обязательно по очереди)
* Под 2 вопрос подойдет картинка парка с выделением вайфая
* Под 3 отдыхающий человек либо залипший в телефоне или читающий статью в интернете
* Под 4 картинка с интервью либо замок с личными данными (тут можно сделать концепт проводов – подключаться от пользователя к правильным ответам)
* Под 5 можно картинку где придумывается пароль 3 (можно как нибудь выделить что правильных ответов несколько)