**Тест на проверку знаний приемов распознавания опасностей**

**при использовании интернета**

***Инструкция:*** *Выберите один правильный вариант ответа на каждый вопрос.*

Вопрос №1. Что такое фишинг?

* А) Попытка украсть личные данные путем рассылки писем якобы от известных компаний.
* Б) Распространение вирусов через вложения электронной почты.
* В) Мошенничество, связанное с распространением спама.
* Г) Взлом аккаунтов пользователей социальной сети.

Вопрос №2. Назовите признак сомнительного письма:

* А) Оно отправлено знакомым человеком.
* Б) Содержит грамматические ошибки и стилистически некорректно написано.
* В) Письмо приходит с рабочего почтового адреса вашей организации.
* Г) Сообщение содержит поздравление с праздником.

Вопрос №3. Опасно ли давать незнакомым людям доступ к своей камере ноутбука?

* А) Нет, это абсолютно безопасно.
* Б) Да, существует риск слежки и похищения личных данных.
* В) Доступ разрешен, если собеседник утверждает, что работает представителем технической поддержки.
* Г) Это допустимо лишь в закрытых чатах социальных сетей.

Вопрос №4. Зачем рекомендуется включать двухфакторную аутентификацию?

* А) Она ускоряет вход в аккаунт.
* Б) Позволяет экономить трафик интернета.
* В) Уменьшает вероятность взлома аккаунта даже при краже основного пароля.
* Г) Помогает быстрее восстановить забытый пароль.

Вопрос №5. Что означает фраза "Социальная инженерия"?

* А) Техническое обслуживание компьютерных сетей.
* Б) Создание мобильных приложений для повышения социального статуса.
* В) Психологические методы манипулирования пользователями ради достижения цели (например, хищения информации).
* Г) Оптимизация интерфейсов популярных сайтов.

Вопрос №6. Безопасно ли подключаться к общественным Wi-Fi-сетям без VPN?

* А) Абсолютно безопасно — такие сети защищены протоколами шифрования.
* Б) Рискованно, поскольку данные легко перехватываются третьими лицами.
* В) Рекомендуется только в общественных местах, где много посетителей.
* Г) Безопасно, если сайт использует HTTPS-протокол.

Вопрос №7. Почему опасно загружать программы с неофициальных сайтов?

* А) Они могут содержать вирусы или шпионские модули.
* Б) Официальные сайты требуют платную подписку.
* В) Пользователь лишается возможности оставить отзыв о продукте.
* Г) Загрузка занимает больше времени.

Вопрос №8. Какие последствия возможны при клике на ссылку в SMS-сообщении от неизвестного отправителя?

* А) Перенаправление на легитимный ресурс.
* Б) Возможность выиграть приз или скидку.
* В) Скачивание вируса или трояна на устройство.
* Г) Получение уведомления о необходимости обновления приложения.

Вопрос №9. Стоит ли отвечать на запросы о предоставлении личных данных в мессенджерах от лиц, представляющихся сотрудниками банка?

* А) Всегда стоит сообщать необходимую информацию, ведь банки заботятся о клиентах.
* Б) Никогда нельзя делиться такими данными вне официальных каналов связи банка.
* В) Ответьте, если вас попросили прислать паспортные данные для подтверждения личности.
* Г) Предоставляйте данные, если собеседник убедил вас, что информация необходима срочно.

Вопрос №10. Когда лучше всего обновить программное обеспечение своего компьютера?

* А) После появления сообщений о новых уязвимостях.
* Б) Сразу же после выхода новой версии программы.
* В) Обновления нужны редко, раз в полгода достаточно.
* Г) По запросу службы технической поддержки вашего провайдера.

Правильные ответы:

1. **А**
2. **Б**
3. **Б**
4. **В**
5. **В**
6. **Б**
7. **А**
8. **В**
9. **Б**
10. **Б**