

- 1. Какие данные пользователя НЕ интересуют киберпреступника?**
 - a) Адрес электронной почты
 - b) Номер телефона
 - c) Личная переписка «ВКонтакте»
 - d) Посты в Instagram
 - e) Им может пригодиться все перечисленное. И еще что-нибудь
- 2. Вы получаете электронное письмо: интернет-магазин предлагает вам получить скидку 20%. Вы переходите по ссылке и видите на сайте форму, где требуется войти в аккаунт Instagram. Что будете делать?**
 - a) Наберу логин и пароль. Мне как раз нужно кое-что из ассортимента этого магазина.
 - b) Подозрительная история. Войду в аккаунт в другом окне, набрав адрес соцсети вручную. Если не поможет, откажусь от скидки...
- 3. Какой из этих паролей лучше всего использовать в учетной записи?**
 - a) k@tya1986
 - b) ivanoFF1
 - c) n0_cyber*Crime%
- 4. Что такое утечка данных?**
 - a) Это когда кто-то узнал о вас что-то плохое и пишет об этом в Интернете.
 - b) Это когда логины и пароли пользователей с какого-то сайта попадают в руки преступников или в открытый доступ в Интернете.
- 5. Что из перечисленного поможет защитить личные данные в Facebook?**
 - a) Ограничение доступа к информации из профиля
 - b) Надежный пароль
 - c) Запрет для посторонних на просмотр списка друзей
 - d) Все перечисленное полезно
- 6. Как сделать так, чтобы ваш профиль «ВКонтакте» видели только друзья?**
 - a) Закрыть профиль
 - b) Не добавлять незнакомых людей, это же очевидно!
 - c) Включить двухфакторную аутентификацию
- 7. Пользователи Instagram, которым вы писали сообщения, могут видеть, когда вы заходили в соцсеть. Это можно изменить?**
 - a) Да, отображение информации о вашей активности можно отключить
 - b) Нет, можно только ограничивать доступ к странице и запрещать отправлять сообщения
- 8. Twitter использует данные своих пользователей для персонифицированной рекламы. Это правда?**

- a) К сожалению, да
 - b) Нет, конечно — что там этой информации, почти что и нет
- 9. Есть ли в «Одноклассниках» двухфакторная аутентификация и надо ли ее включать?**
- a) Есть, просто называется по-другому: «двойная защита»
 - b) Может, и есть, но включать ее незачем
 - c) Нет, но если бы была, стоило бы включить
- 10. Как пользоваться голосовым помощником и не слить конфиденциальные данные?**
- a) Установить надежное защитное решение
 - b) Запретить ему доступ к микрофону
 - c) **Использовать его по назначению, не болтать «за жизнь» и без необходимости не упоминать личной информации**
 - d) Каждый раз в начале разговора с помощником просить не передавать этот разговор третьим лицам
- 11. Чтобы защитить Apple ID понадежнее...**
- a) Задам для него пароль в 5–6 знаков
 - b) Попрошу знакомых ввести их Apple ID на моем устройстве — если его украдут, злоумышленники не смогут угадать, где именно мой
 - c) Введу его на телефонах всех друзей. И сохраню везде пароль, для верности
 - d) **Включу двухфакторную аутентификацию**
- 12. Как называется возможность mail.ru, которая пригодится при регистрации в интернет-магазинах и на других площадках, склонных рассылать спам, — та, что позволяет создать дополнительный адрес, письма на который будут попадать в отдельную папку, а не во «Входящие»?**
- a) Такой функции нет, вы меня пытаетесь обмануть
 - b) «Автоответчик»
 - c) «Спаму нет!»
 - d) «Анонимайзер»
- 13. Вы не дома, трафик на вашем смартфоне кончился, а вам нужно срочно зайти в рабочую почту и отправить письмо коллеге. Что будете делать?**
- a) Просто подключусь к бесплатному Wi-Fi (зайду в «Макдоналдс», например) да отправлю письмо
 - b) **Найду бесплатный Wi-Fi, но перед тем как им пользоваться, включу VPN**
- 14. Что такое файлы cookie и зачем их используют интернет-компании?**
- a) Это файлы, отвечающие за настройку стилей на веб-страницах
 - b) Это файлы с информацией о версии браузера: компании собирают с их помощью статистику о том, кто каким браузером пользуется

- c) Это файлы, позволяющие сайтам узнавать пользователей при повторном посещении: компании хранят в них личные настройки пользователей и отслеживают по ним историю посещений

15. Как зайти на сайт так, чтобы рекламщики не проследили за вами?

- a) Использовать только Internet Explorer или Chrome, а не какие-нибудь малоизвестные браузеры
- b) Включить режим «Инкогнито» в браузере
- c) Использовать только защищенный домашний Wi-Fi

16. Какие персональные данные будут интересны киберпреступнику?

- a) Учетные данные электронной почты
- b) Данные банковской карты
- c) Все вышеперечисленное может быть интересно киберпреступнику
- d) Логин и пароль к развлекательным порталам
- e) Переписки и фотографии в соц. сетях

17. У смартфонов нет физической клавиатуры. Значит ли это, что кейлоггер не сможет записать ввод пароля в интернет-банке на смартфоне?

- a) Нет, кейлоггер действует и на смартфонах
- b) Да, смартфон полностью защищен от записи ввода паролей
- c) Да, но для смартфонов разработаны другие специальные зловреды

18. Какое из перечисленных действий кибербезопасно?

- a) Открытие файла pdf из письма от незнакомого адресата
- b) Передача данных банковской карты по телефону
- c) Скачивание пиратской версии фильма на проверенных торрентах
- d) Отключение антивируса на время установки новой программы
- e) Скачивание игры с официального сайта разработчика

19. Выберите все способы, которые помогут сделать интернет-платежи безопаснее.

- a) Использование виртуальной карты с ограничением суммы
- b) Использование технологии «Безопасные платежи»
- c) Использование зарплатной карты для интернет-покупок
- d) Установка антивируса

20. У меня нет большого числа подписчиков на Facebook, поэтому киберпреступник не станет взламывать мой аккаунт. Так?

- a) Конечно, на вашей странице нечего делать
- b) Нет, любой аккаунт может принести выгоду киберпреступнику

21. Подруга, с которой вы давно не общались, пишет вам

«ВКонтакте». Она просит перейти по ссылке, чтобы ей начислили бонусы в каком-то интернет-магазине. Вы переходите по ссылке, и вас просят ввести логин и пароль от аккаунта «ВКонтакте». Ваши действия?

- a) Введу, мне не трудно подружке помочь.
- b) **Она мне сто лет не писала, и тут кидает ссылку.**

Подозрительно это. Не буду ничего нигде вводить.

22. Вы подключились к бесплатному Wi-Fi в «Макдоналдсе» и вдруг вспоминаете, что забыли заплатить за Интернет дома. Вчера был последний день. Оплачиваем сейчас?

- a) **Да, сейчас. Вот только VPN включу.**
- b) Конечно, прямо сейчас, уже ввожу пароль от интернет-банка.
Дома-то интернет уже не работает!
- c) Подожду до дома, оттуда безопаснее.

23. Для чего нужна двухфакторная аутентификация?

- a) **Чтобы плохие парни не влезли в мой аккаунт, даже если узнают мой пароль.**
- b) Чтобы разработчики могли больше доверять пользователям сервисов.
- c) Чтобы разработчики могли выманить у пользователя не только e-mail-адрес, но и номер телефона или отпечаток пальца

24. Вы включаете компьютер и вместо рабочего стола видите сообщение о том, что ваши данные зашифрованы и вам нужно заплатить выкуп, чтобы их вернуть. Заплатите?

- a) Заплачу, и как можно быстрее – там же вся моя жизнь!
- b) **Попробую вернуть свои файлы как-нибудь иначе – вдруг получится...**

25. Где НЕ стоит хранить резервные копии файлов с вашего компьютера?

- a) В сетевом хранилище NAS.
- b) на флешке или на внешнем диске – вдруг потеряется или сломается?
- c) **На диске C, в папке «Мои документы».**
- d) В облаке – небезопасные они.

26. Что можно настроить при автоматическом резервном копировании?

- a) Можно выбрать, в какое время и как часто делать бэкап.
- b) Можно выбрать файлы, которые нужно забэкапить.
- c) Можно выбрать место для бэкапа.
- d) Можно пароль на бэкап поставить.
- e) **Все перечисленное.**

27. Для чего киберпреступникам может понадобиться ваш компьютер?

- a) **Чтобы спам рассылать, чужие сайты атаковать и биткойны майнить.**
- b) Чтобы поиграть с него в майнкрафт.
- c) У меня богатая коллекция мемов.