Защити свои данные[1]

Введение

Марина, ученица 7 класса, активно пользуется социальными сетями и участвует в различных онлайн-конкурсах. Однажды ей пришло сообщение от незнакомого человека, представившегося сотрудником популярного онлайн-магазина. В сообщении говорилось, что Марина выиграла ценный приз, но для его получения необходимо подтвердить свои личные данные, включая номер банковской карты и CVC-код. Марина очень обрадовалась выигрышу и чуть было не отправила свои данные, но вовремя вспомнила о правилах безопасности в интернете, которые обсуждались в школе. Она решила посоветоваться со своим старшим братом – будущим специалистом по кибербезопасности. Он внимательно прочитал сообщение и усмехнулся:

– Это классика. Мошенники часто высылают такие «выигрыши» – на самом деле это фишинг.

– А что это? – удивилась Марина.

– Фишинг– от английских слов password и fishing. Это как рыбалка на пароли – тебе забрасывают наживку, а ты, если не заметишь подвоха, сам отдашь свои данные.

Брат на секунду задумался и добавил:

– Вообще, многие термины в области цифровой безопасности заимствованы из английского и несут в себе образ или метафору. Но как бы схема мошенничества ни называлась, ни в коем случае нельзя передавать свои личные данные незнакомым людям.

[1] Задание разработано в рамках ОНТП «Научно-методическое обеспечение формирования функциональной грамотности обучающихся в образовательном процессе» («Функциональная грамотность», № ГР 20212108).

Задание 1 / 7

Прочитайте введение. Затем приступите к выполнению задания.

Какие признаки указывают на то, что сообщение, полученное Мариной, скорее всего, является мошенническим?

Для ответа выберите вариант «верно» или «неверно».

Признаки	Верно	Неверно
Сообщение пришло от незнакомого человека		
В сообщении говорится о крупном выигрыше		
Просят сообщить личные данные, включая номер банковской карты и CVC-код		
Предложение слишком выгодное, чтобы быть правдой		
Сообщение пришло в социальной сети, а не по электронной почте		

Задание 2 / 7

Какие меры предосторожности должна соблюдать Марина при использовании социальных сетей, чтобы минимизировать риск стать жертвой мошенников?

Ответ запишите.

Задание 3 / 7

Воспользуйтесь введением.

Сопоставьте типы мошенничества в интернете с их описанием:

Тип мошенничества	Описание
1. Фишинг	А. Рассылка ложных сообщений о выигрышах, требующих предоплату для получения приза.
2. Фарминг	Б. Получение доступа к логинам и паролям пользователей.
3. «Нигерийские письма»	В. Перенаправление пользователей на поддельные веб-сайты без их ведома.

Задание 4 / 7

Выделите во введении фрагмент, содержащий совет, который помог Марине избежать мошенничества.

Задание 5 / 7

Какие действия следует предпринять, если вы подозреваете, что стали жертвой мошенников в интернете?

Выберите нужный вариант ответа:

- Сообщить об этом в милицию
- Заблокировать банковскую карту (если данные были скомпрометированы)
- Изменить пароли от всех своих учетных записей
- Все вышеперечисленное

Объясните свой ответ.

Задание 6 / 7

Представьте, что Марина решила создать информационный плакат для своей школы о безопасности в интернете. Выберите три наиболее важных правила, которые, по вашему мнению, должны быть включены в этот плакат:

Отметьте три варианта ответа.

- ☐ Не сообщайте свои личные данные незнакомым людям
- ☐ Используйте сложные и разные пароли для разных учетных записей
- ☐ Не переходите по подозрительным ссылкам
- ☐ Регулярно обновляйте антивирусное программное обеспечение
- ☐ Не верьте всему, что видите в интернете
- ☐ Всегда советуйтесь со взрослыми, если у вас возникли сомнения

Объясните свой выбор.

Задание 7 / 7

Какие факторы, на ваш взгляд, способствуют распространению мошенничества в интернете?

Отметьте в таблице нужные варианты ответа.

Факторы	Верно	Неверно
Анонимность в интернете		
Доверчивость пользователей		
Недостаточная осведомленность о правилах безопасности		
Стремление к легкой наживе		
Недостаточное внимание к безопасности со стороны интернет-провайдеров		