Внешний курс. Этап 2

Защита ПК/телефона

Буллер Т.А.

13 мая 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Буллер Татьяна Александровна
- студент направления Бизнес-информатика
- Российский университет дружбы народов

Вводная часть

Объект и предмет исследования

- Инструменты и методы шифрования дисков
- Пароли и методы их защиты
- Вредоносные программы различных типов

Цели и задачи

- Получение и закрепление на практике знаний о базовых мерах обеспечения безопасности электронных устройств и основных ошибках пользователей.

Выполнение контрольных заданий

Шифрование диска

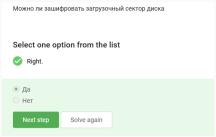

Рис. 1: Задание 1

Зашифровать можно любой раздел диска, в том числе загрузочный, чем нередко пользуются злоумышленники.

Шифрование диска

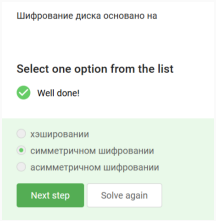

Рис. 2: задание 2

Шифрование диска основано на симметричном шифровании с использованием постоянного ключа: пароля.

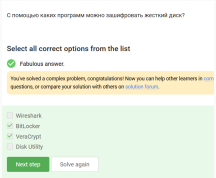

Рис. 3: Задание 3

Wireshark - инструмент анализа сетевого трафика, Disk Utility - утилита для работы с дисками, но не для их шифрования. Наиболее популярные инструменты для шифрования дисков - VeraCrypt и BitLocker.

Пароли

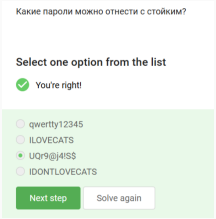

Рис. 4: Задание 4

Пароли 1, 2 и 4 не содержат специальных символов и представляют собой достаточно предсказуемые фразы в одном регистре, что делает их уязвимыми даже к перебору без словаря. Наиболее безопасен из представленных третий пароль.

Пароли

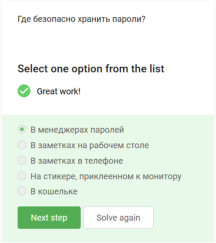

Рис. 5: Задание 5

Пароли должны храниться в специализированных приложениях, но не в местах, где к ним может получить доступ третье лицо.

Рис. 6: Задание 6

Капча - “проверка на человека”, защищает от автоматизированных атак.

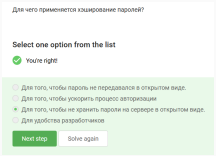

Рис. 7: Задание 7

Хэширование паролей применяется для шифрования паролей и усложнения получения доступа к учетным записям конкретных пользователей, если злоумышленник получил доступ к базе данных сервера.

Пароли

Рис. 8: Задание 8

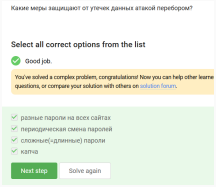

Рис. 9: Задание 9

Все перечисленное (как длинные/сложные пароли, так и регулярное их обновление, разные пароли на всех сайтах и капча) защитят пользователя в случае, если сервер подвергнется атаке перебором. Длинные пароли подобрать сложнее, регулярное обновление и разные пароли на сайтах позволяют избежать совпадения со слитыми базами, капча - убедиться, что войти пытается человек, а не брутфорс-скрипт.

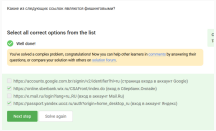

Рис. 10: Задание 10

Фишинговыми являются 2 и 4 ссылки, так как сайт, под который они пытаются мимикрировать, является доменом не второго, а третьего уровня (основными являются соответственно wix.ru и ucoz.ru).

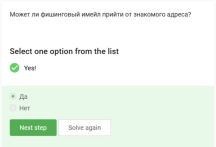

Рис. 11: Задание 11

Фишинговое письмо может прийти со знакомого адреса, если владелец аккаунта был взломан.

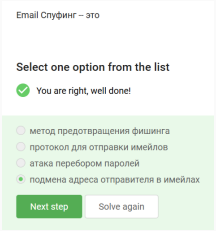

Рис. 12: Задание 12

Спуфингом называется подмена адреса. Атака перебора паролей - брутфорс, протоколов электронной почты имеется великое множество, точно как и методов предотвращения фишинга.

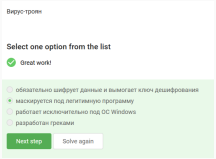

Рис. 13: Задание 13

Троян - вирус, маскирующийся под легитимную программу. Название идет от легенды о троянском коне, однако вирус вовсе не обязательно работает только с отдельной операционной системой или разработан греками.

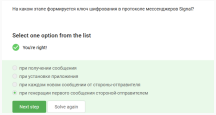

Рис. 14: Задание 14

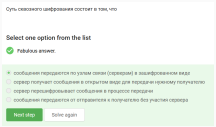

Рис. 15: Задание 15

Суть сквозного шифрования состоит в том, что сообщение не расшифровывается на сервере и недоступно в открытом виде никому, кроме отправителя и получателя.

Выводы

Выводы

Получены и закреплены на практике знания о базовых мерах обеспечения безопасности электронных устройств и основных ошибках пользователей.