

Міністерство освіти і науки України
Сумський державний університет
Наукове товариство студентів, аспірантів,
докторантів і молодих вчених СумДУ

ПЕРШИЙ КРОК У НАУКУ

Матеріали
ІХ студентської конференції
(Суми, 25 лютого 2018 року)



Суми
Сумський державний університет
2018

КІБЕРБЕЗПЕКА: ЗАХИСТ ВІД ФІШИНГУ

Нечепоренко І.Д, *студент*; СумДУ, ННІ БТ “УАБС”, гр. ЕК-61а

У наш час стрімко розвиваються Інтернет-технології і розширюється кібер-простір. Паралельно цьому збільшується вірогідність стати об'єктом злочинних дій шахрая. У даній роботі розглядається один із актуальних видів кіберзагроз під назвою “фішинг”. Фішинг – це різновид шахрайства, метою якого є отримання доступу до конфіденціальної інформації користувача.

Метою роботи є дослідження питань захисту користувачів Інтернет від фішингу.

В листах з фішинговими посиланнями часто вказуються назви відомих сайтів, фінансових організацій, валютних бірж, сервісів Google Docs або Dropbox. Наприклад, в цих повідомленнях пропонуються користувачам вигідні фінансові пропозиції, для отримання яких потрібно ввести особисті ідентифікаційні дані. Шахраї використовують не тільки способи розсилки листів на електронні адреси, але й імітацію спливаючих вікон з системними повідомленнями, дублікати веб-сайтів з єдиною метою – отримання даних банківських карт, акаунтів з криптовалютою та ін.

Для захисту від фішингу пропонується дотримуватися таких рекомендацій: не відкривати листи та не завантажувати вкладення від невідомих адресатів; не відповідати на спам; увімкнути блокування спливаючих вікон у браузері; отримані листи від незнайомих бажано відкривати в Google Docs або Etherpad; рекомендовано перевіряти файли та посилання на сайті VirusTotal на наявність вірусів та шкідливих програм; не відкривати посилання в чатах; уважно використовувати скорочені веб-адреси сайтів; при отриманні листів від служб “технічного обслуговування”, не слідувати їх інструкціям, доки не переконаєтесь в надійності джерела. До надійних способів захисту також відносять шифрування електронних листів за допомогою програми PGP.

Проведене дослідження дозволяє зробити висновок, що дотримання запропонованих рекомендацій дозволить захистити себе, комп'ютер, особисту інформацію, гроші від фішингових кіберзлочинців.

Керівник: Яценко В.В. к.т.н., доцент.