УДК [004.85:004.056](043.2)

Марчук В. О.
Салієва О. В.

АНАЛІЗ ВИКОРИСТАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ФІШИНГУ

Вінницький національний технічний університет

Анотація. *У даній роботі досліджено можливість використання методів машинного навчання для виявлення фішингу. Розглянуто різновиди фішингових атак. Проаналізовано основні типи алгоритмів машинного навчання. Описано процес навчання та оцінювання моделі. Визначено переваги використання машинного навчання для виявлення фішингу.*

Ключові слова: Інформаційна безпека, захист інформації, машинне навчання, фішинг, соціальна інженерія, аналіз даних.

Abstract. *This paper examines the possibility of using machine learning methods to detect phishing. Types of phishing attacks are considered. The main types of machine learning algorithms are analyzed. The process of learning and evaluating the model is described. The advantages of using machine learning for phishing detection have been identified.*

Keywords: Information security, data protection, machine learning, phishing, social engineering, data analysis.

Вступ

Фішинг – це форма кібератаки, яка полягає в шахрайському використанні електронної пошти, соціальних мереж та інших каналів зв'язку, має потенціал для викрадення особистої інформації, фінансових та конфіденційних даних. З розвитком технологій зловмисники вдосконалюють свої методи, роблячи фішингові атаки все більш досконалими та складними для виявлення. Традиційні методи боротьби з фішингом стають все менш ефективними. Тому виникає потреба в нових, більш адаптивних методах. Сьогодні завдяки стрімкому розвитку технологій набирає популярності машинне навчання (ML), яке пропонує перспективний підхід до виявлення фішингу. ML-моделі можуть навчатися на великих обсягах даних, щоб виявляти складні закономірності, які відрізняють фішингові повідомлення від звичайних.

Результати дослідження

Соціальна інженерія – це метод маніпулювання людьми, щоб вони розкрили конфіденційну інформацію або виконали дії, які їм можуть нашкодити. Зловмисники використовують психологічні прийоми, щоб обдурити людей і змусити їх зробити те, що їм потрібно [1].

Атаки соціальної інженерії змушують людей поділитись інформацією, якою вони не повинні ділитися, завантажувати програмне забезпечення, яке вони не повинні завантажувати, відвідувати веб-сайти, які вони не повинні відвідувати, надсилати гроші злочинцям або робити інші помилки, які ставлять під загрозу їхню особисту чи організаційну безпеку.

Електронний лист, який надійшов (як здається) від довіреного колеги із запитом на конфіденційну інформацію, голосова пошта з погрозами, яка нібито надійшла від податкової служби – це лише кілька прикладів соціальної інженерії. Оскільки соціальна інженерія використовує психологічну маніпуляцію та використовує людську помилку або слабкість, а не технічну або цифрову вразливість системи, її іноді називають «зламом людини».

Кіберзлочинці часто використовують тактику соціальної інженерії, щоб отримати особисті дані або фінансову інформацію, зокрема облікові дані для входу, номери кредитних карток, номери банківських рахунків і номери соціального страхування. Вони використовують викрадену інформацію для крадіжки особистих даних, що надає їм змогу робити покупки за чужі гроші, подавати заявки на отримання кредитів від імені іншої особи тощо [1].

Фішинг – це онлайн-шахрайство, спрямоване на крадіжку особистих даних, таких як паролі, номери кредитних карток та банківські реквізити. Зловмисники розсилають фейкові email-повідомлення або текстові повідомлення, які здаються невинними, щоб обдурити людей і змусити їх перейти за посиланням або ввести свої дані на фейковому веб-сайті [2].

Розглянемо різновиди фішингових атак [2]:

– спірфішинг. Цільові атаки на конкретних людей або організації;

– масовий фішинг. Розсилка однакових повідомлень великій кількості людей;

– фейкові веб-сайти. Створення фейкових веб-сайтів, які схожі на легальні веб-сайти, щоб обдурити людей і змусити їх ввести свої дані;

– фармінг. Перехоплення трафіку, щоб перенаправити людей на фейкові веб-сайти.

Машинне навчання (ML) – це наука про алгоритми, які можуть навчатися на даних без явного програмування. Ці алгоритми шукають закономірності в даних, щоб робити прогнози або приймати рішення [3].

Виділяють три основні типи алгоритмів машинного навчання [4]:

– навчання з учителем. Модель навчається на наборі даних, що містить як ознаки, так і цільову змінну. Наприклад, модель може навчатися на наборі даних зображень котів і собак, де ознаками є пікселі зображення, а цільовою змінною – клас ("кіт" або "собака");

– навчання без учителя. Модель навчається на наборі даних, що містить лише ознаки. Наприклад, модель може навчатися на наборі даних про транзакції з кредитними картками, щоб виявити шахрайські транзакції;

– навчання з підкріпленням. Модель навчається в середовищі, отримуючи винагороду за правильні дії та штрафи за неправильні дії. Наприклад, модель може навчатися грати в шахи, отримуючи винагороду за перемогу та штрафи за поразку.

Для розуміння процесу навчання моделі, коротко проілюструємо його на рис. 1 [4].

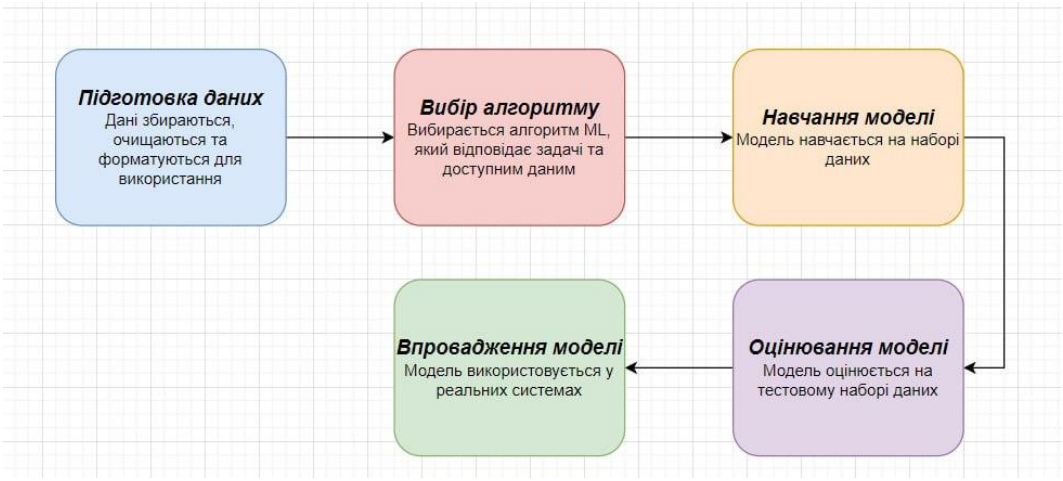

Рисунок 1 – Короткий опис процесу навчання та оцінювання моделі

Враховуючи усі переваги та стрімкий розвиток машинного навчання із зростанням кількості фішингових атак варто розглянути можливість його використання задля виявлення фішингу.

Переваги використання машинного навчання для виявлення фішингу:

– висока точність. ML-моделі можуть бути навчені з високою точністю виявляти фішингові веб-сайти, мінімізуючи кількість помилкових спрацювань;

– адаптивність. ML-моделі можуть адаптуватися до нових методів фішингу, що робить їх більш стійкими до змін у цій сфері;

– можливість виявлення складних атак. Моделі машинного навчання можуть виявляти складні фішингові атаки, які використовують соціальну інженерію та інші методи для обману людей;

– автоматизація. ML-моделі можуть автоматизувати процес виявлення фішингу, що звільняє час та ресурси для інших завдань.

Обмеження використання машинного навчання для виявлення фішингу:

– необхідність великих наборів даних. Для навчання ML-моделей потрібні великі набори даних, що містять інформацію про фішингові та легальні веб-сайти;

– використання ресурсів. Деякі ML-алгоритми можуть бути занадто об’ємними, що може обмежувати їх практичне використання через брак комп’ютерних потужностей;

– можливість упередженості. ML-моделі можуть бути упередженими, якщо дані, на яких вони навчаються, не є репрезентативними для реального світу.

Важливо знати про обмеження машинного навчання та вживати заходів для їхнього подолання. Наприклад, важливо використовувати репрезентативні набори даних для навчання ML-моделей та постійно їх оновлювати.

Для того щоб використати машинне навчання для виявлення фішингових атак необхідно пройти усі кроки проілюстровані на рисунку 1:

– збір даних. Створення наборів даних, що містять інформацію про фішингові та легальні веб-сайти;

– розробка алгоритмів. Вибір та адаптація алгоритмів машинного навчання, які підходять для виявлення фішингу;

– навчання та оцінювання моделей. Навчання ML-моделей на наборах даних та оцінювання їхньої ефективності;

– впровадження моделей. Інтеграція моделей машинного навчання в реальні системи для захисту від фішингу;

– моніторинг та оновлення. Постійний моніторинг та оновлення ML-моделей для адаптації до нових методів фішингу.

Таким чином, машинне навчання має значний потенціал для покращення виявлення фішингу. ML-моделі можуть бути більш точними, адаптивними та стійкими до нових методів фішингу, ніж традиційні методи.

Однак важливо пам'ятати, що ML не є панацеєю. Для досягнення найкращих результатів важливо використовувати репрезентативні набори даних, постійно оновлювати моделі та поєднувати машинне навчання з іншими методами захисту та виявлення фішингу.

Висновок

Варто зазначити що фішинг постійно еволюціонує, тому важливо використовувати адаптивні та гнучкі методи для його виявлення. Машинне навчання ідеально підходить для вирішення цієї задачі. Воно стає ключовим інструментом у боротьбі з фішингом. Завдяки своїй точності, адаптивності, автоматизації та швидкості, ML-моделі можуть значно поліпшити захист людей та організацій від онлайн-шахрайства. Завдяки новим технологіям, таким як машинне навчання, можна значно зменшити шкоду, завдану фішингом, і зробити Інтернет безпечнішим місцем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is social engineering? [Електронний ресурс] / Bart Lenaerts-Bergmans // crowdstrike.com – 2023 – Режим доступу до ресурсу: https://www.crowdstrike.com/cybersecurity-101/social-engineering/
2. Phishing and Communication Channels. A Guide to Identifying and Mitigating Phishing Attacks. 1st Ed. / Gunikhan Sonowal – Apress, 2022. – 15p.
3. What is machine learning and how does it work? In-depth guide [Електронний ресурс] / Linda Tucci // techtarget.com – 2023 – Режим доступу до ресурсу: https://www.techtarget.com/searchenterpriseai/definition/machine-learning-ML
4. Machine Learning Algorithms [Електронний ресурс] / Machine Learning Tutorial // geeksforgeeks.com – 2023 – Режим доступу до ресурсу: https://www.geeksforgeeks.org/machine-learning-algorithms/

Марчук Валерія Олегівна – студентка групи 2КІТС-20б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: valerymarchuk2103@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Marchuk Valeriia O. – student of 2KITS-20b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: valerymarchuk2103@gmail.com

Supervisor: ***Saliieva Olha V.*** – Doctor of Philosophy (PhD) in specialty 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, email: salieva8257@vntu.edu.ua