

Засіб для перевірки QR-кодів на наявність фішингових загроз

Вінницький національний технічний університет

Анотація

Сучасні технології полегшують процес обміну інформацією. Одним з найпопулярніших інструментів для швидкого доступу до онлайн-ресурсів є QR-коди. Вони широко використовуються в маркетингу, мобільних платежах та навігації, зокрема. Але їхня дедалі більша популярність пов'язана з тривожною тенденцією активного використання в фішингових атаках та інших кіберзагрозах, оскільки зловмисники можуть створювати QR-коди, котрі направляють на шкідливі веб-сайти, незаконно збираючи персональні дані або встановлюючи шкідливе програмне забезпечення. У цій роботі описано основні принципи виявлення фішингових загроз у QR-кодах, існуючі підходи до їх перевірки та програмне забезпечення, яке дає змогу аналізувати URL-адреси, закодовані в QR-кодах.

Ключові слова: QR-код, фішингові атаки, кібербезпека, аналіз URL, захист користувачів, розпізнавання QR-кодів, алгоритми виявлення загроз, кіберзлочинність, фішингові сайти.

Abstract

Modern technologies facilitate the process of information exchange. One of the most popular tools for quick access to online resources is QR codes. They are widely used in marketing, mobile payments, and navigation, among others. But their increasing popularity is associated with a worrying trend of active use in phishing attacks and other cyber threats, as attackers can create QR codes that redirect to malicious websites, illegally collecting personal data or installing malicious software. This paper describes the basic principles of detecting phishing threats in QR codes, existing approaches to their verification, and software that allows you to analyze URLs encoded in QR codes.

Keywords: QR code, phishing attacks, cybersecurity, URL analysis, user protection, QR code recognition, threat detection algorithms, cybercrime, phishing sites.

Вступ

У сучасному цифровому світі QR-коди стали невід'ємною частиною повсякдення. Вони широко застосовуються для швидкого доступу до веб-ресурсів, оплати товарів і послуг, аутентифікації користувачів та інших завдань, що потребують миттєвого обміну інформацією. Завдяки зручності та універсальності, QR-коди набули популярності в комерційній сфері, медицині, логістиці та навіть державних установах. Проте, поряд з перевагами, зростає і ризик їх застосування у зловмисних цілях. Кіберзлочинці активно використовують QR-коди для проведення фішингових атак, спрямованих на викрадення персональних даних, фінансової інформації та встановлення шкідливого програмного забезпечення на пристрої користувачів.

Однією з основних загроз є те, що люди не мають можливості візуально перевірити, на який веб-ресурс веде QR-код до його сканування. Це створює ідеальні умови для атак, коли зловмисники маскують шкідливі посилання під легітимні або створюють підроблені QR-коди, що ведуть на фішингові сайти[1]. Більшість користувачів не задумуються над потенційними ризиками та без вагань сканують коди, що може призводити до компрометації їхніх облікових записів, крадіжки особистих даних або фінансових втрат.

Метою цієї роботи є розробка програмного засобу, який дає змогу здійснювати автоматичну перевірку QR-кодів на наявність фішингових загроз, аналізуючи URL-адреси з використанням сервісів Google Safe Browsing та VirusTotal[2]. Запропонований метод забезпечує високий рівень захисту користувачів від потенційних атак і сприяє підвищенню інформаційної безпеки під час роботи з QR-кодами.

Результати дослідження

У ході дослідження було створено програмний інструмент для перевірки QR-кодів на виявлення фішингових небезпек. Він автоматично аналізує URL-адреси, вбудовані у QR-коди, та оцінює їх безпечність до відкриття. З огляду на збільшення кіберзагроз, що стосуються застосування QR-кодів у фішингових атаках, розробка такого інструменту є важливим завданням у сфері інформаційної безпеки. Запропоноване рішення базується на використанні сучасних методів аналізу та виявлення небезпек, зокрема на інтеграції з сервісами Google Safe Browsing і VirusTotal. Це дозволяє суттєво підвищити рівень безпеки користувачів, які взаємодіють із QR-кодами.

Функціональність програмного засобу передбачає декілька основних етапів обробки QR-кодів, починаючи зі зчитування, аналізу та перевірки на предмет потенційних небезпек. Алгоритм роботи програми починається з розпізнавання QR-коду. Це може бути реалізовано із зображення, завантаженого користувачем. Після вдалого розпізнавання видобувається закодована інформація, яка найчастіше містить URL-адресу. Саме на цьому етапі реалізується основна функція безпеки – перевірка отриманого посилання на наявність потенційних загроз.

Перевірка здійснюється шляхом надсилання запитів до двох незалежних сервісів кібербезпеки: Google Safe Browsing і VirusTotal. Google Safe Browsing використовує власні алгоритми для ідентифікації небезпечних веб-сайтів, аналізуючи їхню історію та поведінку. Цей сервіс визначає, чи міститься URL-адреса в базі відомих фішингових або шкідливих сайтів. VirusTotal, своєю чергою, перевіряє адресу за допомогою більш як 70 антивірусних механізмів, що дозволяє провести більш детальний аналіз ресурсу. Отримані результати обробляються програмним засобом, після чого користувач отримує вичерпну інформацію щодо безпеки QR-коду та рекомендації щодо подальших дій.

Розроблений інструмент буде корисним як для окремих осіб, так і для організацій, що прагнуть захистити своїх працівників від кіберзагроз, що виникають при використанні QR-кодів. Його можна інтегрувати у мобільні програми або розширення для браузерів, що дасть змогу автоматично перевіряти QR-коди перед відкриттям, зменшуючи ризики фішингових атак. До того ж можливе впровадження системи автоматичного сповіщення користувачів про підозрілі посилання, що підвищить їхню обізнаність у питаннях кібербезпеки.

Відтак, результати дослідження підтверджують ефективність запропонованого способу перевірки QR-кодів на наявність фішингу. Впровадження такого підходу дозволяє суттєво зменшити ризик компрометації особистої інформації та фінансових втрат, що є важливим в сучасному цифровому світі. Подальше покращення програмного засобу та розширення його функцій сприятиме ще більшій ефективності захисту користувачів від потенційних кіберзагроз, що робить даний напрямок досліджень перспективним та актуальним для майбутніх розробок у сфері інформаційної безпеки.

Висновки

Запропонований засіб дозволить захистити користувачів через аналіз QR-кодів на предмет фішингових ознак перед їх використанням. Це підвищить рівень захисту інформаційної безпеки користувачів та зменшить ризики викрадення даних. Наступні удосконалення можуть бути направлені на впровадження методів машинного навчання для підвищення точності аналізу фішингових посилань, а також на розширення бази відомих загроз через використання технологій спільного аналізу великих обсягів даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. QR Code Security Issues: A Guide To Safe Scanning in 2024 [Електронний ресурс] – Режим доступу: <https://scanova.io/blog/qr-code-security-issues/>
2. Phishing Attacks: A Recent Comprehensive Study [Електронний ресурс] – Режим доступу: <https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full>
3. Google Safe Browsing API Documentation [Електронний ресурс] – Режим доступу: <https://developers.google.com/safe-browsing>
4. A systematic review and research challenges on phishing cyberattacks [Електронний ресурс] – Режим доступу: <https://link.springer.com/article/10.1007/s00779-024-01794-9>
5. Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning [Електронний ресурс] – Режим доступу: <https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2024.1428013/full>
6. Hooked: A Real-World Study on QR Code Phishing [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/382492608_Hooked_A_Real-World_Study_on_QR_Code_Phishing
7. PhishHaven—An Efficient Real-Time AI Phishing URLs Detection System [Електронний ресурс] – Режим доступу: <https://ieeexplore.ieee.org/document/9082616>
8. 2025 QR Code Phishing Trends: In-Depth Analysis of Rising Quishing Statistics [Електронний ресурс] – Режим доступу: <https://keepnetlabs.com/blog/2024-qr-code-phishing-trends-in-depth-analysis-of->

[rising-quishing-statistics](#)

9. Hooked: A Real-World Study on QR Code Phishing [Електронний ресурс] – Режим доступу: <https://arxiv.org/pdf/2407.16230>
10. Phishing Classification Techniques: A Systematic Literature Review [Електронний ресурс] – Режим доступу: <https://ieeexplore.ieee.org/abstract/document/9755138>

Шпаковатий Владислав Олександрович — студент групи ІБС-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: shpakovat12@gmail.com

Shpakovatyi Vladyslav Oleksandrovych — student of group 1BS-21b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: shpakovat12@gmail.com

Науковий керівник : Лукічов Віталій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: lukichov.vitalyi@vntu.edu.ua

Supervisor : Lukichov Vitalii Volodymyrovych — Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical, e-mail: lukichov.vitalyi@vntu.edu.ua