

Методичні вказівки
до лабораторної роботи №4
«Методи соціальної інженерії. Фішинг»
з навчальної дисципліни вільного вибору
«Основи інформаційної та кібербезпеки»

Зміст практичного заняття: Ознайомитись та дослідити один із типів шкідливого програмного забезпечення – фішингові застосунки на прикладі фішингових WEB-ресурсів. Навчитися проводити аналіз URL-адрес хостів, робити попередні висновки щодо безпечності ресурсів мережі Інтернет.

Загальні відомості

Соціальна інженерія – це сукупність методів несанкціонованого доступу до інформації або систем зберігання інформації без використання технічних засобів. Методи засновані на використанні слабкостей людини і є дуже ефективними. Психологічною передумовою застосування методів соціальної інженерії є така особливість людської психіки як когнітивні упередження. Через це надійність комп'ютерної системи є не вищою ніж надійність її оператора. Зловмисник отримує інформацію, наприклад, шляхом збору інформації про службовців об'єкту атаки, за допомогою звичайного телефонного дзвінка або шляхом проникнення в організацію під виглядом її службовця. Зловмисник може подзвонити працівникові компанії (під виглядом технічної служби) і вивідати пароль, пославшись на необхідність вирішення невеликої проблеми в комп'ютерній системі.

Основна тактика соціальної інженерії – за допомогою психологічних методів (наприклад, спілкуючись начебто від імені сервісної компанії чи банку) переконати користувача розкрити інформацію особистого характеру (паролі, номери кредитних карток тощо).

У рамках соціоінженерного підходу вразливості людини тлумачаться як її слабкості, потреби, манії (пристрасті), захоплення. Маніпулювання ними дозволяє отримати несанкціонований доступ до інформації. Як наслідок, це призводить до нової моделі її поведінки, створення сприятливих умов реалізації загроз безпеці інформації і, як наслідок, зменшенню здатності систем захисту інформації протидіяти їх впливові (рис. 1). Це відображається в таких формах як, наприклад, шахрайство, обман, афера, інтрига, містифікація, провокація. Використанню кожної з означених форм маніпулювання передуює визначення її змісту шляхом ретельного планування, організування та контролювання.

З огляду на рис. 1, використання соціоінженерного підходу передбачає цілеспрямований вплив на свідомість (підсвідомість) людини проти волі, але за його згодою.

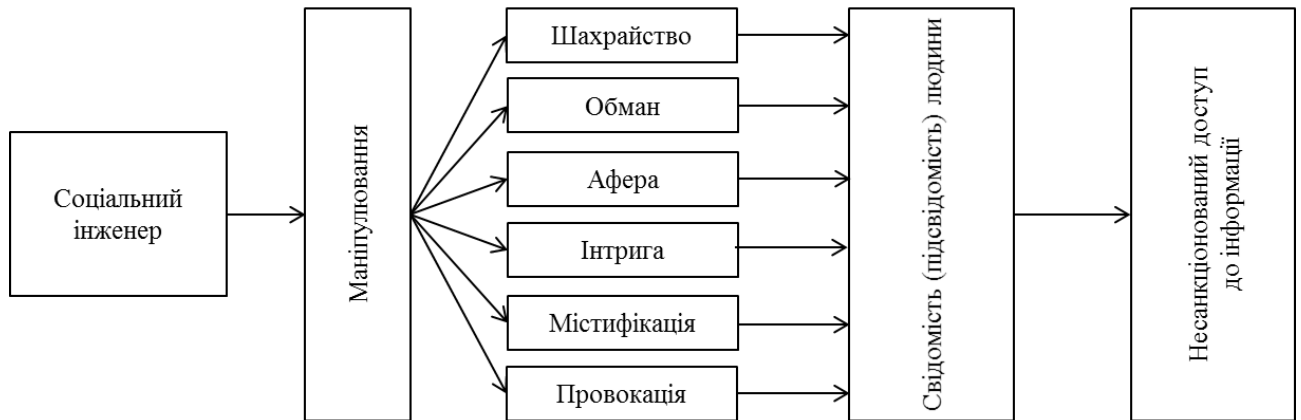


Рисунок 1 – Використання соціоінженерного підходу

Такий вплив дозволяє управляти поведінкою, наприклад, керівництва, адміністратора, користувачів через слабкості, інтереси, потреби, схильності, переконання, звички, психічний та емоційний стан.

Техніки соціальної інженерії

Всі техніки соціальної інженерії засновані на особливостях прийняття рішень людьми.

Претекстинг (Pretexting) – це дія, відпрацьована за заздалегідь складеним сценарієм (претекстом). В результаті ціль (жертва) повинна видати певну інформацію, або вчинити певну дію. Цей вид атак застосовується зазвичай по телефону. Найчастіше ця техніка включає в себе більше, ніж просто брехню, і вимагає будь-яких попередніх досліджень (наприклад, персоналізації: з'ясування імені співробітника, які він обіймав посади і назви проектів, над якими він працює), з тим, щоб забезпечити довіру об'єкта атаки.

Фішинг (Phishing) – масове розсилання електронної пошти великій групі адресатів. Ознайомлення з електронними листами спонукає їх до, наприклад, відкриття вкладення до листа, переходу за посиланням на веб-сторінку. Його метою є виманювання у довірливого або неуважного персоналу комп'ютерної системи персональних даних.

Фармінг (Pharming) – перенаправлення користувачів сайту на інший, підроблений сайт для отримання їх логіну та паролю. Це досягається завдяки розповсюдженню електронної пошти серед користувачів, наприклад, соціальних мереж, онлайн-банкінгу, поштових веб-сервісів. Фармінг може проводитися або шляхом зміни файлу hosts на комп'ютері жертви, або шляхом використання вразливості в програмному забезпеченні DNS-сервера. DNS-сервери – це комп'ютери, що відповідають за перетворення імен Інтернету в їх реальні IP-адреси. Скомпрометовані DNS-сервери іноді називають «отруєними». Фармінг вимагає незахищеного доступу до цільового комп'ютера, наприклад, до зміни домашнього комп'ютера клієнта, а не корпоративного бізнес-сервера.

Смішинг (Smishing) – отримання інформації шляхом масового розсилання SMS повідомлень з посиланням на веб-ресурси або з реквізитами організацій (наприклад, фінансових). Внаслідок цього здійснюються відповідні дії, наприклад, дзвінок до банку для перевірки стану рахунку з зазначенням конфіденційних даних: номеру картки, терміну дії.

Вішинг (Vishing) – отримання інформації шляхом входження в довіру під час розмови через IP-телефон. При цьому порушення конфіденційності здійснюється завдяки викладенню прохання у повідомленні зателефонувати на певний міський номер. Наприклад, вести номер карти, паролі, PIN-коди, коди доступу або іншу інформацію.

Спір фішинг (Spear Phishing) – надсилання листа електронної пошти конкретному адресату (наприклад, керівнику, адміністраторові, користувачеві), що спонукає його до обов'язкового перегляду та відповіді на отриманий лист. Цільові атаки мають великий успіх, тому що вони ретельно підготовлені.

Вейлінг (Whaling) – надсилання листа електронної пошти представнику керівництва організації, що спонукає його до обов'язкового перегляду та відповіді на отриманий лист. Інформація від керівника буде завжди більш цінною ніж від звичайного співробітника. В даному випадку підроблений сайт має велику важливість, оскільки представляє певного клієнта організації. Найчастіше фішингових лист складається як суперечність з клієнтом або офіційна проблема, і має виглядати як справжнє бізнес-листування.

Clone phishing (фішинг-клонування) – тип атаки, при якій фішер клонує вихідне повідомлення, але вкладене в нього посилання замінює на зловмисне. Для цього використовується раніше перехоплене повідомлення і за шаблоном створюється точно таке ж, підробляється відправник. Можливо буде потрібне пояснення чому користувач отримав друге таке саме повідомлення. Як правило такою причиною може бути повторна відправка оригіналу або оновлена версія.

Зворотня соціальна інженерія.

Метою зворотньої соціальної інженерії є змусити ціль саму звернутися до зловмисника за «допомогою». З цією метою зловмисник може застосувати такі техніки:

Диверсія: Створення неполадки на комп'ютері жертви.

Реклама: Зловмисник підсовує жертві оголошення виду «Якщо виникли неполадки з комп'ютером, зателефонуйте за таким-то номером».

Фішинг

Фішинг – це атака на основі соціальної інженерії, яка здійснюється через слабкості в кібербезпеці для обману користувачів з метою крадіжки їх логінів, паролів і грошових коштів. Техніки фішингу досить численні і складні, серед яких такі, які спонукають користувача перейти за посиланням на зловмисний сайт. Не існує універсального визначення фішингу та досі їх існує велика кількість.

Кількість і різноманітність визначень фішингу вказує на складність цього типу атак.

Згідно з сервісом PhishTank Company: фішинг – це спроба вкрати інформацію про людину, використовуючи електронну пошту. Іноді фішингові атаки посиляються на сайти, які є підробкою реальних сайтів організацій, банків і у користувача складається враження, що він потрапив на реальний сайт цієї організації.

Інше визначення звучить так: «Під фішинговою сторінкою розуміється будь-яка веб-сторінка, яка без дозволу заявляє, що діє від імені третьої сторони з метою збити з пантелику користувачів в скоєнні дії, яку користувач може довіряти тільки справжньому агенту третьої сторони.»

Сервіс Anti-Phishing Working Group (APWG) описує фішинг як кримінальний механізм, який використовує як соціальну інженерію, так і технічні прийоми для крадіжки особистих даних користувачів і облікових даних фінансових рахунків.

Виходячи з усіх перерахованих вище визначень можна сказати що, по-перше, фішингова атака може відбуватися з будь-якого електронного каналу зв'язку, по-друге, атакуючий переконує жертву вчинити дії, і, по-третє, атакуючий отримує від цього особисту вигоду.

Отже, фішинг – це комп'ютерна атака, яка передає людям повідомлення соціальної інженерії через електронні канали зв'язку, щоб переконати їх виконати певні дії в інтересах зловмисника.

Згідно зі звітом від сервісу Anti-Phishing Working Group (<https://apwg.org/trendsreports/>) за останній квартал 2021 року:

- У грудні 2021 року APWG зафіксувала 316 747 атак, що стало найвищим місячним підсумком за всю історію звітності APWG.
- З початку 2020 року кількість фішингових атак зросла втричі.
- Фінансовий сектор був найбільш поширеною жертвою фішингу в четвертому кварталі – 23,2% усіх атак. Атаки на Software-as-a-Service (SaaS) та провайдерів веб-пошти продовжували бути численними. Фішинг проти криптовалютних цілей – таких як біржі криптовалют і постачальники гаманців — зріс до 6,5% атак.
- З електронних листів, про які повідомляли корпоративні користувачі, 51,8% були фішинговими атаками, пов'язаними з крадіжкою облікових даних, 38,6% були атаками на основі відповідей (наприклад, BEC, 419 і шахрайство з подарунковими картками), а 9,6% – доставкою шкідливого програмного забезпечення.

Фішери використовують безліч методів, щоб обдурити користувачів. Сюди входять доменні імена, вибрані для уникнення виявлення, шифрування, призначене для приспання жертв у фальшивому почутті безпеки, і оманливі адреси електронної пошти, що використовуються для підміни контактів довірених компаній та осіб.

Типи фішинг-атак

Обманні веб-посилання. Найбільш часто використовувана стратегія полягає в тому, що шахраї маскують зловмисне веб-посилання як вказівку на легітимне або довірене джерело. Ці типи фішингових атак можуть приймати будь-яку кількість форм, наприклад, застосування шахрайських URL-адрес, створення піддомену для зловмисного веб-сайту або експлуатація дуже схожих доменів.

Як приклад розглянемо таке: латинська літера I дуже близька до L на стандартних клавіатурах QWERTY, що робить «GOOGIE» дуже схожим на «GOOGLE». У випадку субдоменів зловмисник, який, наприклад, контролює доменне ім'я example.com, може створити субдомени для нього — «www.paypal.example.com». В період президентських виборів у США 2016 року для проведення фішинг-атаки на базі схожих доменів зловмисники використали сайт «accounts-google.com» як клон сайту «accounts.google.com».

Інтернаціональні доменні імена (IDN) також можуть використовуватися для створення заплутано схожих доменних імен, дозволяючи використовувати не-ASCII символи. Візуальні подібності між символами в різних сценаріях, які називаються гомогліфами, застосовують для створення доменних імен, що візуально неможливо диференціювати. Це спонукає користувачів приймати один домен за інший.

Клонування веб-сайтів, підробка та перенаправлення. Веб-сайти, вразливі до атак типу міжсайтовий скриптинг (XSS), використовуються зловмисниками для запису власного контенту на інший веб-сайт. XSS-атака може застосуватися для перехоплення даних, введених на скомпрометованому сайті (включно з ім'ям користувача та паролем), які зловмисники використають пізніше.

Деякі фішингові атаки використовують XSS для створення **вікон, що спливають**, які походять з вразливого веб-сайту, але притому завантажують сторінку, що контролюється зловмисниками. Часто такий тип прихованого перенаправлення відкриває форму для входу з метою збору реєстраційних даних. Через поширення цього типу атаки більшість браузерів тепер показують адресний рядок у вікнах, що спливають.

Голосовий та текстовий фішинг. Для отримання інформації про обліковий запис зловмисники використовують телефонні дзвінки та текстові повідомлення. Спочатку вони надсилають клієнтам банків повідомлення, де стверджують, що їхній обліковий запис заблоковано. Це спонукає користувачів подзвонити на вказаний номер телефону або зайти на веб-сайт, що контролюється шахраями, і залишити конфіденційну інформацію.

Троянський кінь. Ця техніка експлуатує цікавість, або жадібність цілі. Зловмисник відправляє e-mail, що містить у вкладенні важливе оновлення антивіруса, або навіть свіжий компромат на співробітника. Така техніка залишається ефективною, поки користувачі будуть сліпо клікати по будь-яких вкладеннях.

Дорожнє яблуко. Цей метод атаки є адаптацію троянського коня, і полягає у використанні фізичних носіїв інформації. Зловмисник може підкинути інфікований CD, або карту пам'яті, в місці, де носій може бути легко знайдений (коридор, ліфт,

паркінг). Носій підробляється під офіційний, і супроводжується підписом, покликаним викликати цікавість.

Приклад: Зловмисник може підкинути CD, забезпечений корпоративним логотипом і посиланням на офіційний сайт компанії мети, і забезпечити його написом «Заробітна плата керівного складу Q1 2021». Диск може бути залишений на підлозі ліфта, або у вестибюлі. Співробітник через незнання може підібрати диск, і вставити його в комп'ютер, щоб задовольнити свою цікавість.

Кві про кво (*Qui pro Quo* – латинський вираз, який буквально означає *хтось за когось*). Зловмисник може подзвонити за випадковим номером в компанію, і представитися співробітником техпідтримки, запитувати, чи є які-небудь технічні проблеми. У разі, якщо вони є, в процесі їх «рішення» ціль вводить команди, які дозволяють зловмиснику запустити шкідливе програмне забезпечення.

Технічна складова фішингу

- Кодування символів HTML: шифрується HTML-код сторінки, щоб пошукові роботи не змогли виявити ключові слова, що вказують на шкідливий сайт.
- Шифрування вмісту: аналогічно кодуванню HTML, використовується приховування вмісту для запобігання виявлення.
- Блокування перевірки: захищає від пошукових роботів і тих, які шукають фішингові сайти.
- URL-адреси у вкладеннях: приховує шкідливі посилання у вкладеннях, щоб вони не були очевидні.
- Ін'єкції контенту (content injection): впровадження шкідливого контенту на сторінку легітимного веб-сайту для того, щоб приховати справжню природу фішингового сайту.
- Законний хмарний хостинг: використання відомих легальних хмарних провайдерів для розміщення фейкових сайтів.

Зараз практично всі фішингові ресурси використовують цифрові сертифікати для підвищення рівня довіри до них. Згідно Anti-Phishing Working Group (APWG), ще два роки тому назад SSL-сертифікати були тільки у половини фішингових сайтів.

Заходи протидії фішингу

Оскільки фішингові атаки спрямовані на людей, то й основним способом захисту від них буде робота з людьми, яка складається з двох обов'язкових частин:

- **навчання співробітників** навичкам безпечної поведінки при роботі і в повсякденному житті;
- **відпрацювання практичних навичок** безпечної поведінки за допомогою систем, що імітують реальні атаки.

Якщо користувачів навчити, як виявляти ознаки шахрайських електронних листів та час від часу проводити в компанії **таємну імітацію фішингових атак** з

метою перевірки ефективності цього навчання, такі дії забезпечать набагато кращий захист, ніж спеціалізовані програмні рішення.

З технологічної точки зору, варто провести правильне налаштування клієнтів електронної пошти, таких як Microsoft Outlook, адже параметри за замовчанням не є оптимальними для безпеки. Крім того, **інструменти для сканування повідомлень** від сторонніх виробників можуть зменшити ефективність фішингових атак або навіть запобігти їхньому потраплянню до поштових скриньок користувачів.

Також сучасні веб-переглядачі включають так звані служби Безпечного перегляду, які увімкнені вже за замовчуванням. Вони здатні виявляти фішингові атаки й захищати від них користувачів.

PhishTank – це проект від OpenDNS, який допомагає перевіряти сайти, які намагаються проводити фішинг. OpenDNS – це служба, яка дозволяє доменні імена, так і забезпечує блокування веб-сайтів, які підозрюються в якості фішингових доменів.

Щоб допомогти PhishTank, ви можете голосувати за або проти веб-сайтів, представлених в його базі даних. Процес називається перевіркою Phish і доступний в розділі VERIFY A PHISH на веб-сайті. Ви повинні увійти в систему, перш ніж зможете перевіряти сайти.

Ви також можете повідомляти про спроби фішингу по електронній пошті в співтовариство PhishTank. PhishTank просить вас перенаправити такі фішингові листи, оскільки пересилання листів може видалити певну інформацію або змінити заголовки листів. Щоб повідомити щодо фішингових листів в PhishTank, просто перенаправте будь-який підозрілий лист на phishing@phishingtank.com.

На сайті Департаменту кіберполіції України існує сервіс STOP FRAUD (<https://cyberpolice.gov.ua/stopfraud/>). Він також містить інформацію про шахрайські веб-ресурси. Щоб перевірити який-небудь сайт, слід в рядку пошуку ввести його адресу. Список шахрайських ресурсів регулярно оновлюється співробітниками кіберполіції. Джерело – заяви громадян, які звернулися в поліцію у зв'язку з фішингом. Кожен веб-ресурс отримує короткий опис.

Щоб дати українцям можливість перевірити підозрілий сайт, Українська міжбанківська асоціація членів платіжних систем ЕМА склала «чорний список» фішингових сайтів: <https://www.ema.com.ua/citizens/blacklist/>.

Завдання до лабораторної роботи

Завдання А. Пошук фішингових WEB-ресурсів.

1. Знайти і коротко описати у звіті можливі способи атак з використанням соціальної інженерії, певні відомі випадки використання методів соціальної інженерії.

2. Вибрати 10 будь-яких онлайн-фішингових URL-адрес із бази шахрайських сайтів Асоціації ЄМА (<https://www.ema.com.ua/citizens/blacklist/>) або сервісу Phishtank (<http://phishtank.org/>) та знайти і зберегти інформацію про них у таблиці:

- a. дата створення домену (<https://2ip.ua/ua/services/information-service/domain-information>);
- b. дата оновлення домену;
- c. назва реєстратора;
- d. країну IP-адреси (<https://2ip.ua/ua/services/information-service/site-location>).

Приклад:

Таблиця 1.1 - Результати аналізу шахрайських сайтів

| | Сайт | Дата створення домену | Дата оновлення домену | Назва реєстратора | Місцезнаходження IP-адреси домену |
|----|------------------------------|-----------------------|-----------------------|-------------------|-----------------------------------|
| 1. | theaterdram.site | 2021-01-17 | 2021-01-22 | REG.RU, LLC | Україна, Київ |
| 2. | paysend-ua.com | 2021-02-08 | 2021-02-08 | Name.com, Inc. | Франція, Страсбург |
| 3. | novaposhta-safedostavka.site | 2020-11-15 | 2021-01-30 | REG.RU, LLC | не знаходиться |
| 4. | | | | | |
| 5. | | | | | |

Завдання Б. Провести експеримент з дослідження наскільки сильним є вплив соціальної інженерії.

Мета експерименту буде виявити наскільки сильним є вплив соціальної інженерії і як легковажно ми інколи відносимось до фішингових посилок.

Просимо Вас:

1. відправити листа електронною поштою 10-тьом знайомим.
2. надіслати повідомлення у Facebook (Instagram, Viber, Telegram тощо) 10 знайомим, звісно якщо Ви користуєтесь даними соц. мережами чи месенджерами.

Для того, щоб обрати шаблон повідомлення пройдіть тест від компанії Google: <https://phishingquiz.withgoogle.com/>

Приклади повідомлення:

- Привіт, давай сходимо)) <http://faceelbook.com/photo/album/87445>
- Зверни увагу, твій мобільний у відкритому доступі у <http://faceelbook.com/photo/album/87445>

У Вас є два варіанти виконання завдання Б:

1) Запитайте через день у друзів, чи перейшли вони за посиланням. Проаналізуйте зібрані дані у звіті до лабораторної роботи.

2) Створіть сайт для симуляції фішингової атаки, на якому буде оброблятися статистика відвідувань.

Один із способів реалізації другого варіанту приведений нижче:

2.1. Створюємо сайт на платформі heroku.com

- Завантажуємо та встановлюємо git
<https://git-scm.com/download/win>
- Створюємо обліковий запис (акант) на хероку (Heroku – хмарна PaaS-платформа, що підтримує низку мов програмування).
<https://www.heroku.com/>
- Завантажуємо та встановлюємо одну з програм під свою розрядність Windows (<https://devcenter.heroku.com/articles/heroku-cli>)
32x <https://cli-assets.heroku.com/heroku-x86.exe>
64x <https://cli-assets.heroku.com/heroku-x64.exe>

Рекомендовано перезапустити комп'ютер після встановлення всіх програм.

2.2. Завантажуємо сайт

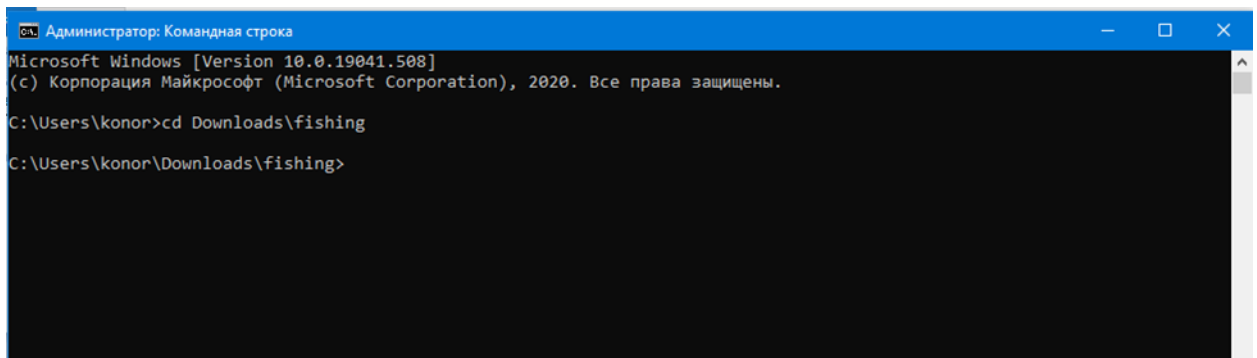
Завантажуємо код з <https://github.com/konorth3/fishing>

Після встановлення відкриваємо командний рядок (ви вже всі вмієте це робити з попередніх робіт).

Переходимо в папку з завантаженим кодом з github.

У моєму випадку це наступна команда

```
cd Downloads\fishing
```

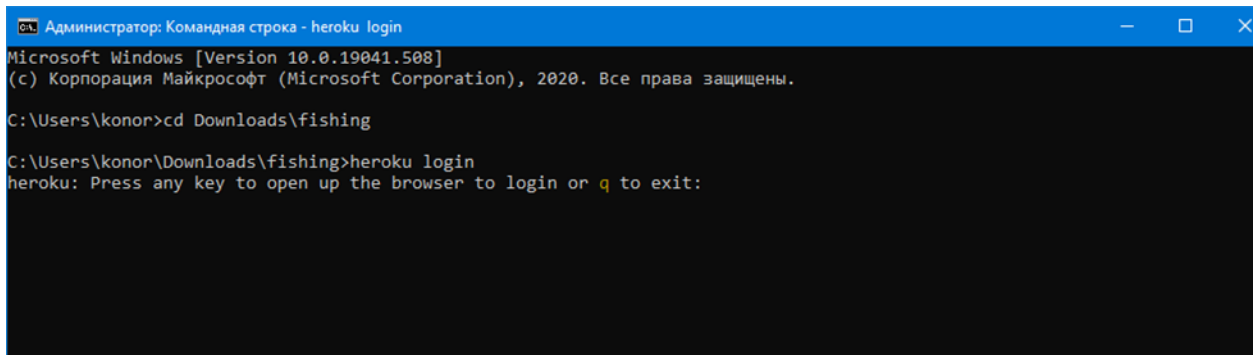


```
Администратор: Командная строка
Microsoft Windows [Version 10.0.19041.508]
(c) Корпорация Майкрософт (Microsoft Corporation), 2020. Все права защищены.

C:\Users\konor>cd Downloads\fishing
C:\Users\konor\Downloads\fishing>
```

Та виконуємо наступну команду

```
heroku login
```



```
Администратор: Командная строка - heroku login
Microsoft Windows [Version 10.0.19041.508]
(c) Корпорация Майкрософт (Microsoft Corporation), 2020. Все права защищены.

C:\Users\konor>cd Downloads\fishing
C:\Users\konor\Downloads\fishing>heroku login
heroku: Press any key to open up the browser to login or q to exit:
```

Нас просять натиснути будь-яку клавішу окрім «q» натискаємо, після цього нас перенаправляє на сторінку heroku де потрібно залогінитись.

Натискаємо кнопку, якщо ми не виходили з акаунту після реєстрації то нас автоматично залогинить і можемо закривати вкладку браузера. Ми повинні побачити приблизно такий текст в командному рядку

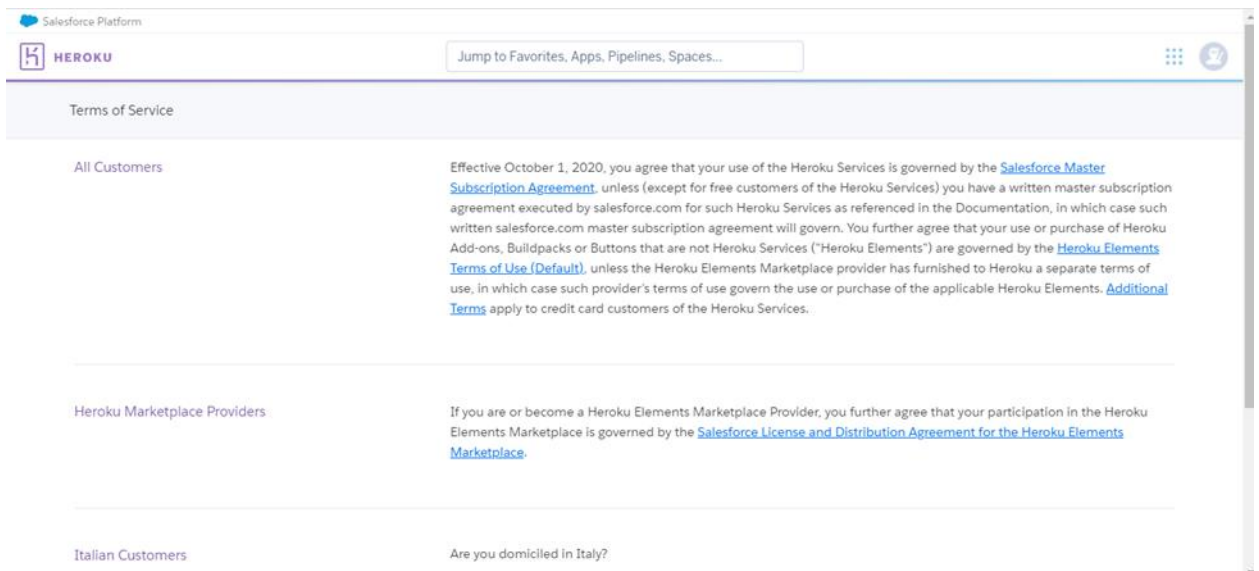
```
Администратор: Командная строка
Microsoft Windows [Version 10.0.19041.508]
(с) Корпорация Майкрософт (Microsoft Corporation), 2020. Все права защищены.

C:\Users\konor>cd Downloads\fishing

C:\Users\konor\Downloads\fishing>heroku login
heroku: Press any key to open up the browser to login or q to exit:
Opening browser to https://cli-auth.heroku.com/auth/cli/browser/4926cb1f-2f30-46ad-9f10-ead3d6b10511?requestor=SFMyNTY.g
2gDbQAAAA45M14yNTMuMjQ4LjI1MW4GAPpvqxJ4AWIAAVGA.kHM1MUaXcKLH5KK4-QQJ6GrpHZbs1KA_fAh9LHD30zY
Logging in... done
Logged in as @gmail.com

C:\Users\konor\Downloads\fishing>
```

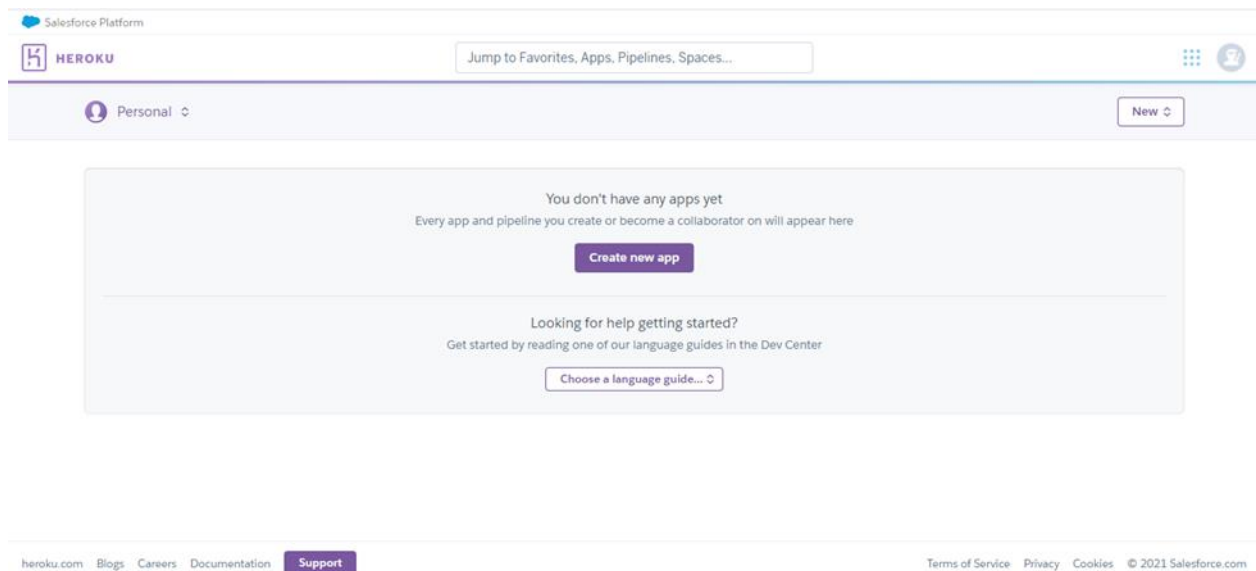
Погоджуємось з політикою компанії.



Натискаємо на піктограму heroku

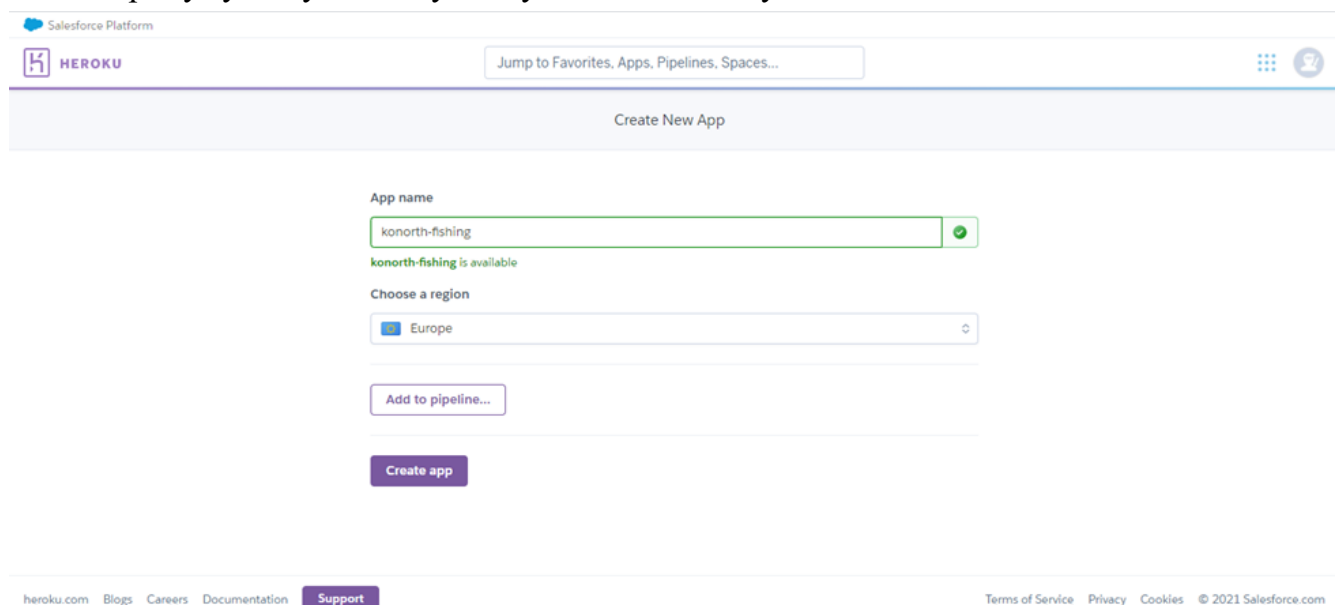


в лівому верхньому куті
бачимо наступне вікно



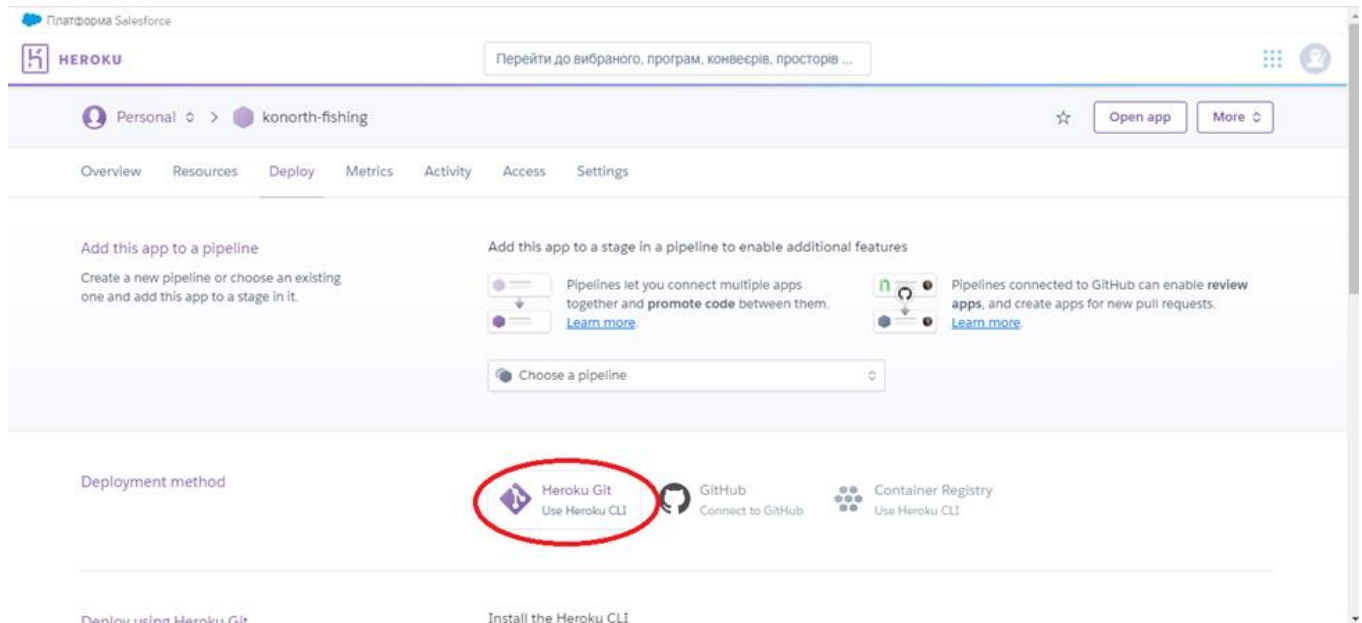
Натискаємо клавiшу «**Create new app**».

Придумуємо унікальну назву для свого сайту.

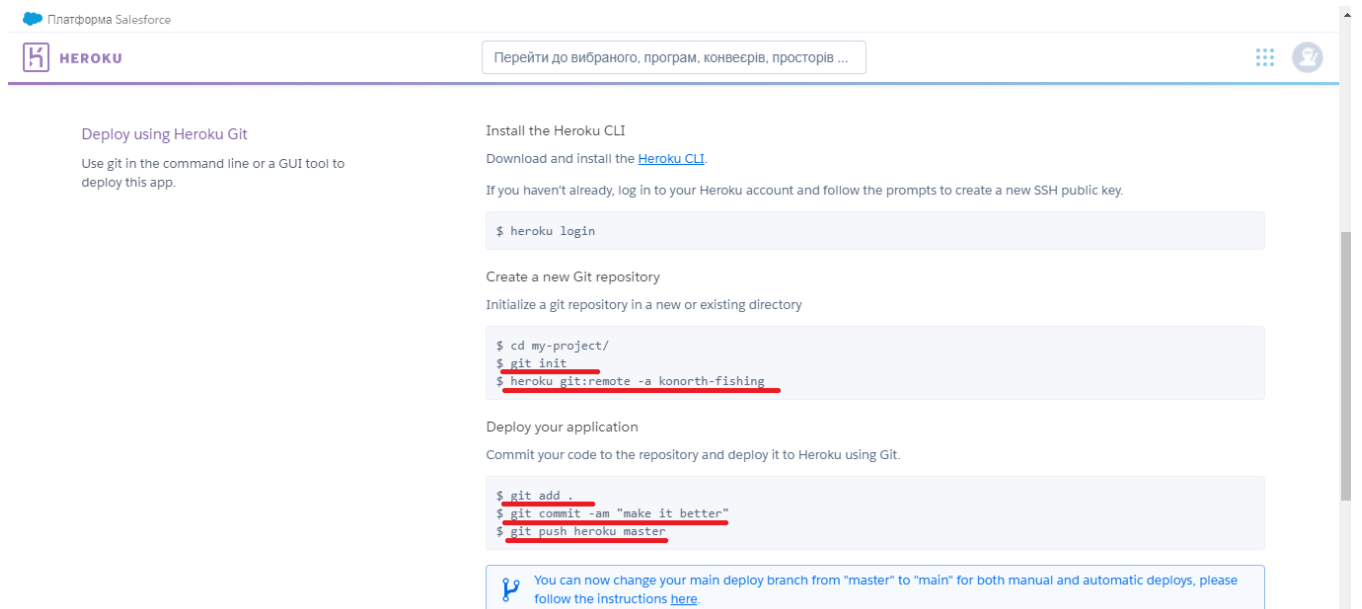


Натискаємо клавiшу «**Create app**».

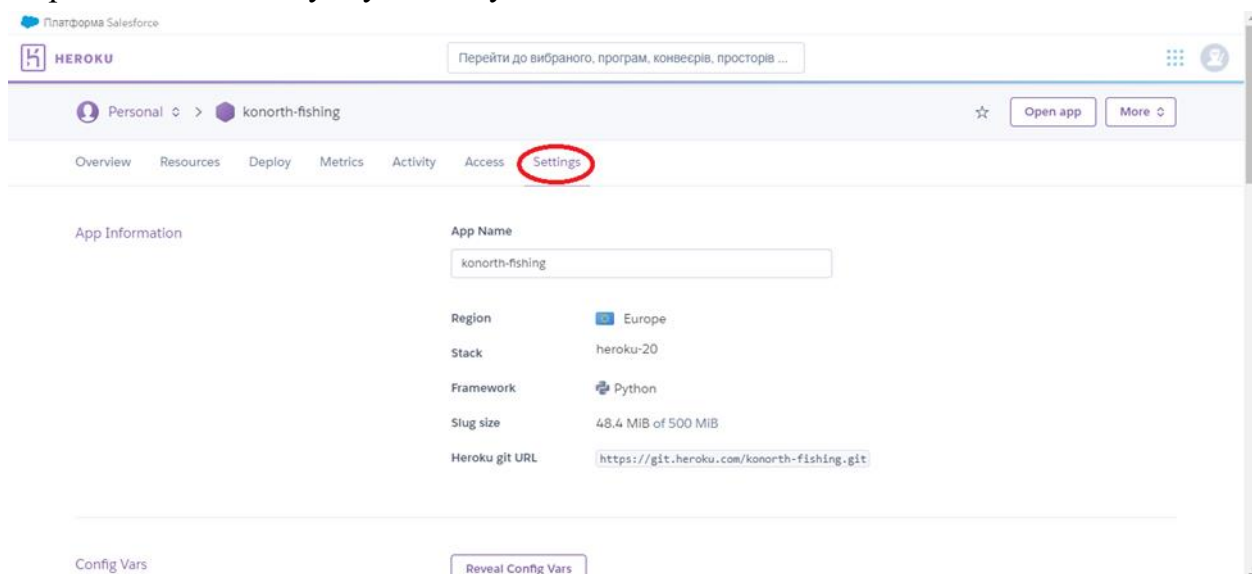
Далі переходимо на наступну вкладку.



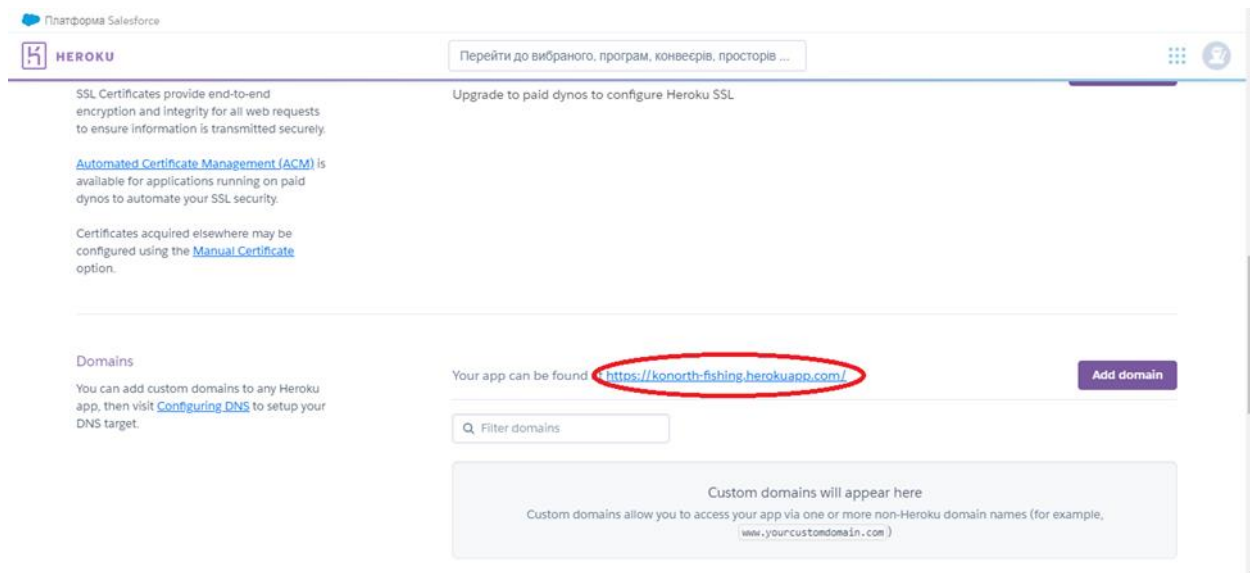
Далі виконуємо підкреслені команди одна за одною. Друга буде у Вас дещо іншою.



Переходимо на наступну вкладку.



Гортаємо нижче до схожого запису.



Виділена адреса буде адресою вашого сайту.

Переходьте за ним. Термінал можна закрити. Політика heroku надає 550 годин в місяць на використання сайту. Якщо вам з якоїсь з причин потрібно більше, можна додати дані про банківську карту, це збільшить ліміт до 1000 годин в місяць. (Використання heroku надалі буде безкоштовним, карта потрібна лише для верифікації вашої особистості). Отже у вас є 550 годин на виконання завдання, після чого немає жодних гарантій про збереження даних та працездатності сайту.

2.3. Налаштовуємо фішинговий сайт

Це наш сайт за допомогою якого ми будемо фішити:

| Konorth3 | | | |
|-----------|---------------|----------------------------|--------------------|
| Посилання | Час створення | Час переходу за посиланням | Створити посилання |
| | | | |

Для початку натисніть на посилання праворуч «Створити посилання»

Вас скерує на поле для реєстрації адміністратора.

Важлива деталь. Пароль та ім'я повинні містити хоча б один символ, їх неможливо буде змінити, скинути або відновити, тому запам'ятайте пароль. В поле адрес потрібно вставити URL вашого сайту.

Konorth3

Зареєструватись

Щоб розлогінітись натисніть на цю область.

Konorth3 & Kon

| Посилання | Час створення | Час переходу за посиланням | Створити посилання |
|-----------|---------------|----------------------------|--------------------|
| | | | |

Для повторного логіна знову скористайтесь полем «Створити посилання»
Буде створений унікальний ідентифікатор, за яким вам потрібно направити свою «жертву».

Konorth3 & Kon

| Посилання | Час створення | Час переходу за посиланням | Створити посилання |
|--|---------------------|----------------------------|--|
| IndHquGOsd74czVoUpnXyg52RRMvU74t1gklTXUs1iba3TjzjCNuoVrxzanWS0vN | 2021-03-08 18:28:15 | не відправлено | <div>Відправлено</div> <div>Видалити</div> |

Після того як ви сформуєте посилання та відправите його комусь натисніть клавішу «відправлено». Поле «Час переходу за посиланням» зміниться, а посилання буде відслідковуватись. При першому переході за ним буде встановлено час, коли ваша «жертва» попалась, а її проінформовано про те, що вона стала жертвою

фішингу. У будь-якому випадку ви можете видалити непотрібне або використане посилання.

Перейдемо до справи. **Як формувати посилання?** Перше що нам потрібно це URL нашого сайту у мене він <http://konorth-fishing.herokuapp.com>

Далі нам потрібно до нього додати наступний рядок
`/i_stole_your_data?key=`

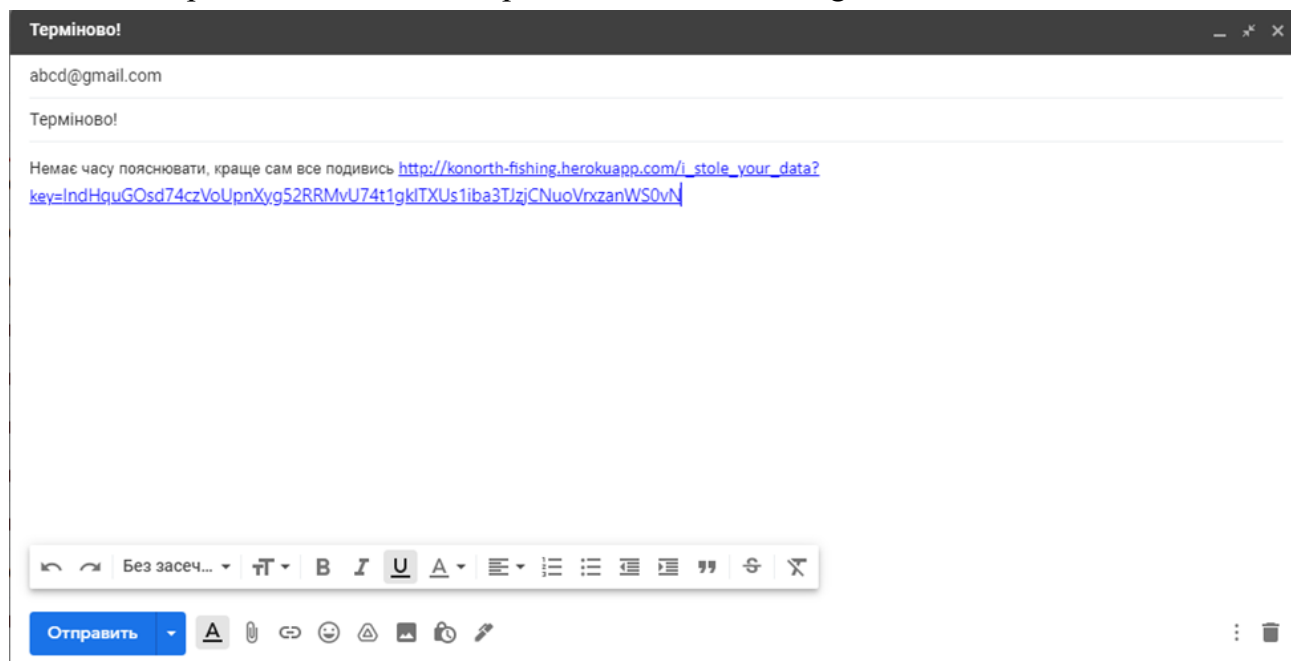
та до нього додати рядок зі стрічки посилання
`IndHquGOsd74czVoUpnXyg52RRMvU74t1gklTXUs1iba3TJzjCNuoVrxzanWS0vN`

В зібраному вигляді ми отримуємо

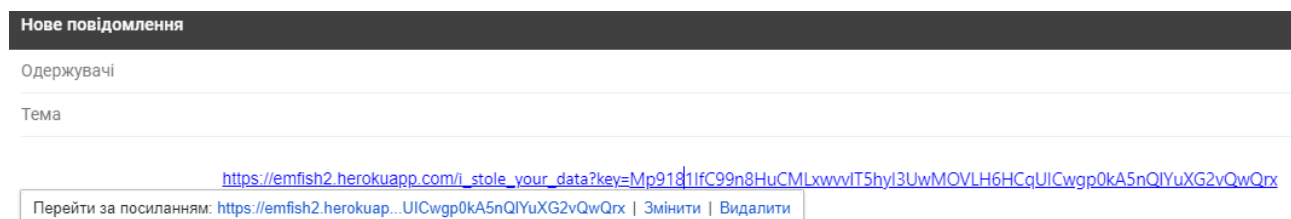
http://konorth-fishing.herokuapp.com/i_stole_your_data?key=IndHquGOsd74czVoUpnXyg52RRMvU74t1gklTXUs1iba3TJzjCNuoVrxzanWS0vN

Таке посилання вам і потрібно замаскувати під щось корисне. Для початку варто потренуватись, і самостійно створити, активувати, сформувати та перейти за ним. Якщо все зробите правильно, то після переходу Ви отримаєте дані про час переходу людини за вашим посиланням.

Ось приклад як це можна зробити за допомогою gmail пошти:



Клікаємо на посилання у тексті нашого фішингового листа, з'явиться кнопка «Змінити». Натискаємо її.



Обираємо пункт «Веб-адреса», в верхнє поле пишемо як має виглядати посилання, в нижньому полі - наше сформоване посилання.

Змінити посилання

Текст для відображення:

Посилання на:
☒ Веб-адреса
☐ Адреса електронної пошти

На яку URL-адресу має спрямовувати це посилання?

[Перевірити посилання](#)
Не впевнені, що вказати в цьому вікні? Спершу знайдіть в Інтернеті сторінку, на яку потрібно зробити посилання посиланням (вам може стати в нагоді [пошукова система](#)). Після цього скопіюйте адресу сторінки з адресного рядка вашого веб-переглядача та вставте її в рядок вище.

Скасувати

Все, наше повідомлення готове до надсилання, при спробі переходу за посиланням, людина потрапить не на Youtube, а до нас.

P.S. Не забудьте активувати посилання одразу після відправлення. Якщо посилання активне – в полі «Час переходу за посиланням» відображено текст «очікую».

Терміново!

abcd@gmail.com

Терміново!

Немає часу пояснювати, краще сам все подивись <https://www.youtube.com/watch?v=Z9W2Xe1Xu8c>

Отправить

Отправить

У звіті про виконання **завдання Б** цієї лабораторної роботи вкажіть реальну кількість відправлених повідомлень та кількість друзів, які перейшли за надісланим посиланням, не поцікавившись у Вас, що це таке.