Модуль: Соціальна інженерія

Практична вправа:
«Аналіз поштового повідомлення»

Навчальна мета заняття: отримати практичні навички аналізу поштового повідомлення.

Час проведення: 1 год. *Місце проведення:* комп'ютерний клас.

Устаткування:
персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено.**

Фішингові повідомлення часто надходять користувачам за допомогою електронної пошти.

Змоделюємо ситуацію, яким чином це може відбуватися та як можна запобігти цьому негативному явищу.

Спершу слід зареєструвати тестову поштову скриньку, на яку будемо одержувати відповідні повідомлення. Після реєстрації електронної поштової скриньки слід надіслати на неї неправдиве повідомлення з підміною заголовка. Для цього можуть бути використані сервіси https://emkei.cz/, https://anonymousemail.me/ тощо. Приклад відповідним чином сформованого листа наведено на рис. 1.

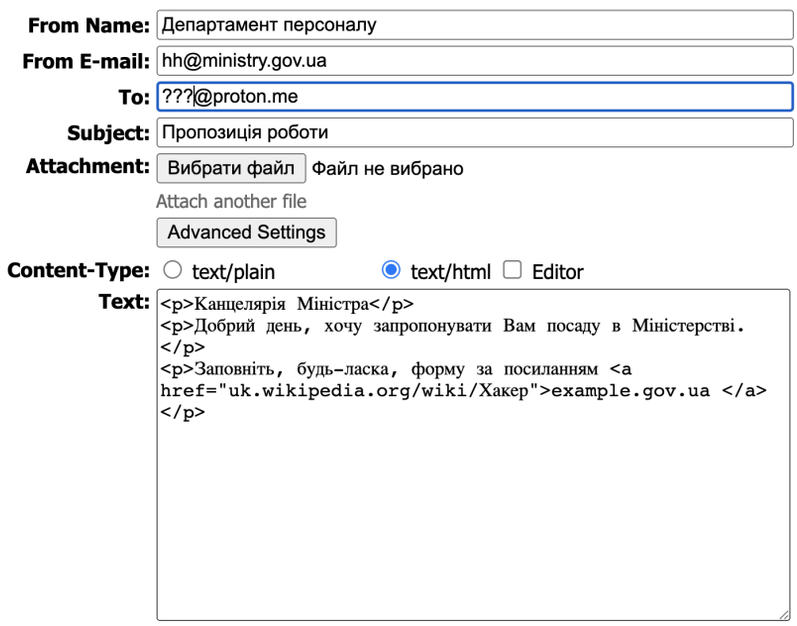

Рис. 1. Відправлення неправдивого повідомлення

У результаті на поштову скриньку надійде лист як на рис. 2.

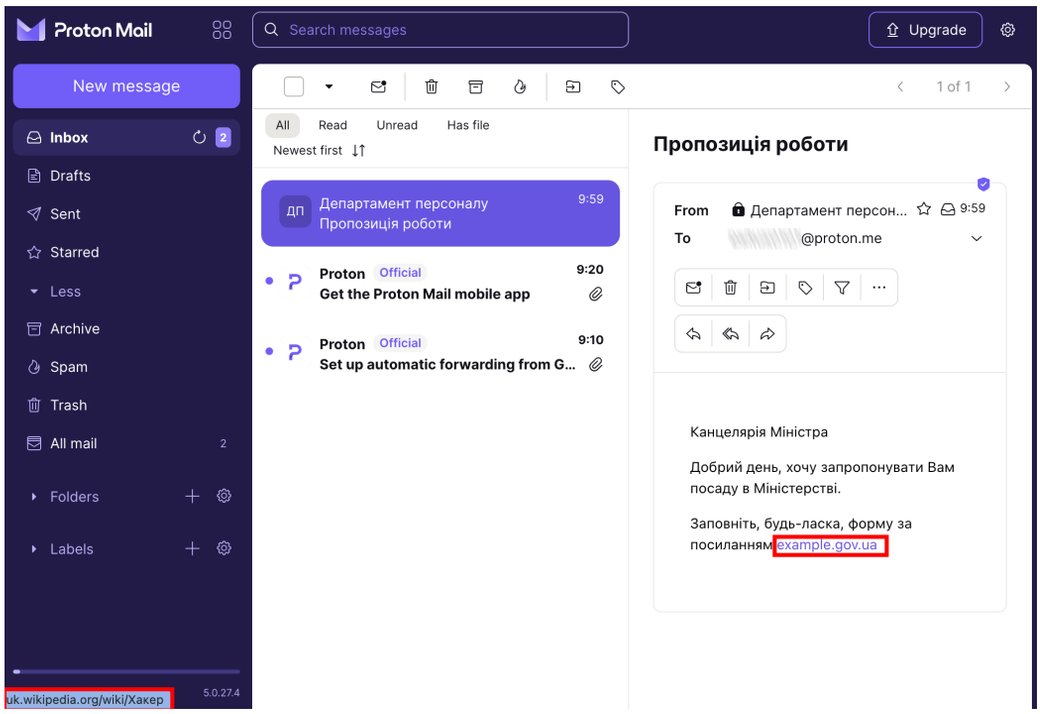

Рис. 2. Повідомлення, що надійшло

Для того, щоб виявити підробку в листі, потрібно дослідити його поштовий заголовок. Для цього слід після відкриття листа натиснути «Переглянути заголовок».

Return-Path: <hh@ministry.gov.ua>
X-Original-To: ???@proton.me
Delivered-To: ???@proton.me
Received: from emkei.cz (emkei.cz [89.187.129.22]) (using TLSv1.3 with cipher
TLS_AES_256_GCM_SHA384 (256/256 bits)
key-exchange X25519 server-signature RSA-PSS (4096 bits) server-digest SHA256)
(No
client certificate requested) by mailin005.protonmail.ch (Postfix) with ESMTPS id
4RYPgY4Bbzz9vNPV for <???@proton.me>; Sun, 27 Aug 2023 06:59:21 +0000 (UTC)
Received: by emkei.cz (Postfix, from userid 33) id 2E8B35849E1; Sun, 27 Aug 2023
08:59:15
+0200 (CEST)
Authentication-Results: mailin005.protonmail.ch; dmarc=none (p=none dis=none)
header.from=ministry.gov.ua
Authentication-Results: mailin005.protonmail.ch; spf=none smtp.mailfrom=ministry.
gov.ua
Authentication-Results: mailin005.protonmail.ch; arc=none smtp.remote-
ip=89.187.129.22
Authentication-Results: mailin005.protonmail.ch; dkim=none
To: ???@proton.me
Subject: =?utf-8?B?0J/RgNC+0L/QvtC30LjRhtGW0Y8g0YDQvtCx0L7RgtC4?=

From: =?utf-
8?B?ItCU0LXQv9Cw0YDRgtCw0LzQtdC90Yig0L/QtdGA0YHQvtC90LDQu9GDIiA8?=
 =?utf-8?B?aGhAbWIuaXN0cnkuZ292LnVhPg==?=
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: hh@ministry.gov.ua
Reply-To: hh@ministry.gov.ua
Content-Type: text/html
Message-Id: <20230827065915.2E8B35849E1@emkei.cz>
Date: Sun, 27 Aug 2023 08:59:15 +0200
X-Rspamd-Server: cp3-mailin-005.plabs.ch
X-Rspamd-Queue-Id: 4RYPgY4Bbzz9vNPV
X-Rspamd-Action: add header
X-Spamd-Result: default: False [8.80 / 25.00]; MISSING_MIME_VERSION(2.00)[];
    MIME_HEADER_CTYPE_ONLY(2.00)[];   PHISHING(2.00)[example.gov.ua->wikipedia.
org];
 HFILTER_FROMHOST_NORES_A_OR_MX(1.50)[ministry.gov.ua]; AUTH_NA(1.00)[];
 MIME_HTML_ONLY(0.20)[]; ONCE_RECEIVED(0.10)[]; FROM_EQ_ENVFROM(0.00)[];
 MIME_TRACE(0.00)[0:~]; RCVD_TLS_LAST(0.00)[]; RCVD_COUNT_ONE(0.00)[1];
 NEURAL_SPAM(0.00)[0.986]; ASN(0.00)[asn:35592, ipnet:89.187.129.0/24, country:CZ];
 R_DKIM_NA(0.00)[]; DMARC_NA(0.00)[ministry.gov.ua]; RCPT_COUNT_ONE(0.00)[1];
    FROM_HAS_DN(0.00)[];   ARC_NA(0.00)[];   HAS_X_PRIO_THREE(0.00)[3];   R_SPF_
NA(0.00)[no SPF
  record]; REPLYTO_ADDR_EQ_FROM(0.00)[]; TO_MATCH_ENVRCPT_ALL(0.00)[]; TO_
DN_NONE(0.00)[];
 HAS_REPLYTO(0.00)[hh@ministry.gov.ua]
X-Spam: Yes
X-Pm-Spam: 0yezJI6cihyJeYR3pi42biOpJJvbmsCIeI1msjN3X3blJp7IjBINIIoj2sUjLIITJ
    o4IjsjgLIBISiQ0TiOx0wiOSPFJUR9FQEVkUUSUN9OSUwjoILJCfiVGZWdfd5maW6yIbeJ
yQE9kU   jI7pBfInh3BcbIS6x4CMzM2cU0OT3zEMMkDy1kDOSNiw1haWf2VZbFmt6ISZm
IzhFjdGv19aYNnI   IZncFZy8IzMDxDgMMICs1JnIIbu91IYWijoIYxWsIZWLXY1RVzcmiiwIbF
Wpj9FbXYIR9yZ2uV9e   Y1WIiojIVVEBRFQVsyIUI1mhfxWa2Y0FdvZWfnIccJHv6IiYCM44Y5
MT9jIMf0XshNmIGdnVJ5b3   ijoIVBVEFRVQyUsINyIniWQaOIi2hVGNjZ0QFhYjITdMNMm
3mJjMDN1QYiYTiSwfcE2iisnOXafN   Bhc36SIbMwSivN2cmciUYsOjjnNIbJ3I6ICZiN14Jy
LCvXBZcQniisnOkTf95TREP0ZXU9IGN9kU   jIbp4wNCiSwXQFkZfNVRTNiAsxOIsjALINnj
IJ3biOwAQ5LjiTkOXwSiGB1U0XFh9fTETEFUUIy6   w0yWjLdBJELCN0ISXF0EfB1UITEh1
BT0iU4SOsIwdIjLCLTJZfUEOk9TRIS6uAzWFMs0hUIkfUxT   TVUTHF0USR6IAuWzsF0M
I1kJfVUTFSNR9PTFZkxTIpjbx4CMSXiwRNSFNF9TS1UFP50X0XUhxfTU   HEFVIpjb04C
MSXiwINTUIV9RRFUEfJVR1QZRVfUEM05TWIS6uAzWVMs0RWIITF9RUFEDS9VRVQJR
9NT1GU5SUIC6uAzWFM91fX0=
X-Pm-Origin: external
X-Pm-Transfer-Encryption: TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256
bits)
X-Pm-Content-Encryption: on-delivery
X-Pm-Spamscore: 6
X-Pm-Spam-Action: inbox
Mime-Version: 1.0

Базовий формат поштових повідомлень (листів, messages) і статей USENET (article) визначається RFC 822 і його «спадкоємцем» RFC 2822. Кожне повідомлення (лист, message, стаття, article) складається з конверта і вмісту. Конверт зберігає адресну інформацію, необхідну для відправлення і передачі повідомлення одержувачеві. Формат конверта визначається середовищем розповсюдження. Для його автоматичного створення може використовуватися інформація зі вмісту повідомлення. Стандарт визначає тільки формат вмісту повідомлення і лише у момент передачі, тобто повідомлення можуть зберігатися абсолютно в іншому форматі. Повідомлення ділиться на рядки і складається з секції заголовків і тіла повідомлення (можливо, порожнього).

Заголовок електронного поштового листа можна дослідити або вручну, або за допомогою програм чи сервісів (рис. 3).

IP Address	93.99.104.210
Country	Czech Republic
Region	-
City	-
ISP	Liberty Global
Organization	Liberty Global
Latitude	50.0848
Longitude	14.4112

Рис. 3. Результат аналізу заголовка поштового листа

Виходячи з даних, наведених в теоретичних відомостях:

1. Зареєструвати поштову скриньку та надіслати тестове повідомлення.
2. Проаналізувати заголовок та тіло листа зі своєї електронної поштової скриньки. Визначити адресу відправника та маршрут руху листа за допомогою сервісів:
https://www.iplocation.net/trace-email, https://mha.azurewebsites.net/, https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=73671c03-950e-4f79-88ee-f78a785b2eef, https://www.ip2location.com/free/email-tracer, https://www.whatismyip.com/email-header-analyzer/.

Приклад. ***«Розшифровка типового заголовка листа»***

Return-path: *******@ukr.net*** *– зворотна адреса, вказана відправником;*
Received: from [212.9.224.21] (port=25 helo=mail-out.iptelecom.net.ua) *– лист отримано від хосту*
mail-out.iptelecom.net.*ua з IP-адресою 212.9.224.21;*
by mx5.mail.ru *– ім'я комп'ютера, який приймав повідомлення;*
with esmtp id 1COINS-000F0L-00 *– комп'ютер, що прийняв повідомлення, надав йому ідентифікаційний номер 1COINS-000F0L-00;*
Tue, 18 Nov 2008 02:14:18 +0300 *– передавання листа здійснювалося у вівторок, 18 листопада 2008 року, о 02:14:18 за часом третього часового поясу, який випереджає Гринвічський часовий пояс на 3 години, звідси «+0300»;*
Received-SPF: none (mx5.mail.ru: 212.9.224.21 is neither permitted nor denied by domain of ukr.net) client-ip=212.9.224.21 *– отримана відповідь на SPF-запит. Технологія SPF (Sender Policy Framework) є одним зі способів ідентифікації відправника електронного листа та надає додаткову можливість фільтрування потоку пошти на наявність у ньому повідомлень зі спамом. За допомогою SPF пошта поділяється на «дозволену» й «заборонену» відносно домена одержувача чи відправника. В цьому випадку поштовий сервер-одержувач mx5.mail.ru здійснив SPF-запит до домена ukr.net, де було отримано відповідь про фактичну відсутність SPF-захисту (дослівно: mx5.mail.ru здійснив SPF-запит до домена ukr.net про наявність у списках IP-адреси 212.9.224.21, на що було отримано відповідь про те, що цю адресу не внесено ані в дозволені, ані в заборонені списки SPF домена ukr.net);*
envelope-from=*@ukr.net*** *– заголовок, який додається до листа деякими поштовими програмами під час доставки кінцевому одержувачу;*
helo=mail-out.iptelecom.net.ua;
Received: from h136.246.159.dialup.iptcom.net ([213.159.246.136]:64011 «HELO copm1» ident: «NO-IDENT-SERVICE[2]» whoson: «s-m-i-t»);
by pechkin.iptelecom.net.ua with SMTP id S358789AbUKAXOS (ORCPT <rfc822;igoset@mail.ru> + 3 others);
Tue, 18 Nov 2008 01:14:18 +0200 *– час, коли одержано лист;*
Message-ID: <021501c4c068$4d89ba20$0200a8c0@copm1> *– процес одержання листа первинним провайдером для подальшого пересилання з ПК, підключеного за допомогою модемного з'єднання (h136.246.159.dialup.iptcom.net). Розшифрування є аналогічним вищевикладеному;*
From: *******@ukr.net*** *– напис на «конверті», від кого лист;*
To: <**@mail.ru>, <**@ukrpost.net>, <@mail.ru>, <**@ukr.net>, <**@yahoo.co.uk>, <**@ok.ru>, <**@yandex.ru>, <****@mail.ru>, <*****@mail.ru>, <**@bk.ru>, *@ukr.net*** *– адреси доставки листа;*
Subject: =?koi8-r?B?8NLFxMzP1sXOycU=?= *– тема листа (у разі заміни кодування тема матиме вигляд напису «Предложение»);*
Date: Tue, 18 Nov 2008 00:52:14 +0200 *– дата та час створення листа (вівторок 2 листопада 2008 р., о 00:52:14 на комп'ютері зі встановленим другим часовим поясом);*
MIME-Version: 1.0 *– версія стандарту, відповідно до якого створено цей лист;*
Content-Type: multipart/alternative *– формат змісту листа. Визначається тип інформації в листі та спосіб її відображення. Зокрема, встановлюється кодування листа, якщо використовується який-небудь національний набір символів;*
boundary=»----=_NextPart_000_0015_01C4C076.3170DA90» *– стандартизація розбивання великих листів на кілька частин. У полі «Content-Type» після значення «multipart/<subtype>» зазначається рядок – унікальний обмежувач фрагментів «boundary=<boundary string>». Потім перед кожним фрагментом пишеться цей рядок з двома мінусами попереду, а в кінці фрагментації – ще один рядок, який завершується такими самими двома мінусами.*
X-Priority: 3 *– пріоритет листа, позначений цифрами.*
X-MSMail-Priority *– нестандартне поле Microsoft – пріоритет листа. Буває «звичайним», «невідкладним» та «не невідкладним». Зазвичай використовуються слова: «Normal», «Urgent», «Non-urgent». Може впливати на швидкість обробки та передачі листа різними проміжними поштовими системами;*
X-Mailer: Microsoft Outlook Express 5.50.4927.1200 *– інформація про поштову програму, яка використовувалася для створення листа;*
X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4927.1200 *– інформація про фірму – виробника програмного забезпечення;*
X-Spam: *Not detected – лист не визначено як спам.*