УДК 004.056.53

Колісніченко О.Ю., Бісюк В.А.
Кіровоградський національний технічний університет

Методи захисту від хакерів при роботі із електронними скриньками

На сьогоднішній день існує безліч методів дистанційної передачі інформації, але найрозповсюдженішим із них електронна пошта.

Ми користуємося нею кожного дня для обміну важливими даними чи повідомленнями із друзями рідними, чи колегам. Однак, цей спосіб не є ідеальним, і що важливіше, він не є абсолютно безпечним.

Основними проблемами із якими зустрічаються користувачі, це віруси, спам та спроби хакерів отримати певну інформацію із листів. Нажаль, на сьогоднішній день, майже непосильною задачею є створення повністю автоматизованої системи захисту від усіх можливих небезпек, тому нерідко користувачеві доводиться самостійно слідкувати за конфіденційністю своєї електронної переписки.

Основні засоби автоматизованого захисту. Відомо, що розробники шкідливого програмного забезпечення є дуже винахідливими, і тому часто для полегшення користувачеві захисту своєї електронної скриньки (а інколи і всього комп'ютера), у різні сервіси електронної пошти встановлюють вбудовані програми для автоматичного пошуку вірусів у повідомленнях.

В основному для цього використовують бази даних анти-вірусних програм таких, як Касперський та DellScience. Це дозволяє легше розпізнавати віруси і попереджати серйозні загрози користувацькій інформації. Але такі системи мають і серйозний недолік – вони можуть сильно сповільнювати роботу серверів, й нерідко цією «прогалиною в безпеці» користуються для проведення ddos-атак й повалення самих поштових сервісів.

Для автоматичного захисту від різноманітних спам-повідомлень існують спеціальні фільтри. Ці фільтри шукають у назві, темі, чи тексті повідомлень певні патерни (слова, словосполучення, а іноді і цілі листи), що вже були позначені користувачами як спам, або занадто часто відправлялися на різні адреси. Ця система є досить ефективною, і успішно відсіює більшість простих спам-повідомлень, але , нажаль, кожного разу, коли створюють новий патерн, потрібен хоча б тиждень щоб його розпізнати і додати то бази даних, тому багато людей все ж потрапляють у пастки злочинців.

Для захисту поштових скриньок від спроб зламу самих авторизаційних даних, розробники використовують різноманітні методи «доповненого рівня безпеки». Такими методами є обмеження спроб введення невірного пароля, прив'язка акаунтів до певних IP-адрес чи комп'ютерів, необхідність підтвердження авторизації через електронні ключі чи телефони. Такий спосіб показав себе досить надійним із технічного боку, але нерідко сам користувач скоює помилки і таким чином порушує власну безпеку.

Основні способи ручного захисту. Зрозуміло, що в багатьох випадках, автоматичних методів захисту недостатньо, часто користувач електронної пошти повинен дотримуватись деяких правил, аби підвищити рівень безпеки своєї інформації.

Для захисту від вірусів, відправлених через електронні листи, достатньо дотримуватись наступних правил :

- Не скачувати файлів, отриманих у листах від недовіреного джерела.
- Не переходити по невідомим посиланням у отриманих повідомленнях (Особливо у спам-повідомленнях!)
- Інколи, вірус може активуватися навіть після простого читання лиса, тому бажано відразу видаляти повідомлення, отримані від невідомих джерел.

Захиститися від вірусів, розповсюджуваних через електронну пошту досить легко, особливо, якщо одночасно користуватись захищеними сервісами електронної пошти та дотримуватись вищеперерахованих правил.

В плані захисту від спам-повідомлень, автоматичні сервіси виконують більшість роботи, але інколи деякі повідомлення все ж проходять через фільтр та потрапляють до вашої скриньки вхідних повідомлень, тому перевіряючи непрочитані листи, і зустрівши ті з них, які мають щонайменші натяки на спробу реклами, або шахрайства, користувач повинен повідомити свій сервіс про належність цього листа до спаму. В більшості сервісів електронних скриньок є для цього спеціальні вкладки, посилання чи просто кнопки.

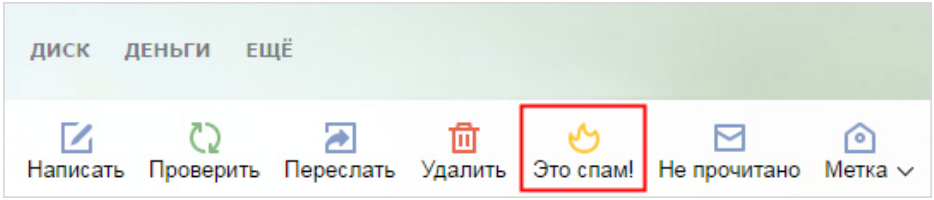

Рисунок 1 – Кнопка повідомлення про спам Яндекс-Пошти.

Коли ж справа стосується захисту власне свого акаунту, основна відповідальність лягає саме на плечі користувача.

Існує величезна кількість правил, що дозволять вам підвищити надійність своєї поштової скриньки, але я перерахую основні із них:

- Тримати авторизаційну інформацію в секреті ВІД УСІХ.
- Запам’ятовувати свій акаунт та пароль від нього, а не залишати собі записки із нагадуваннями, особливо, коли справи стосуються вашого робочого місця.
- Вигадуйте складні паролі, які зможете запам’ятати лище ви, й не використовуйте прямі данні у якості нього (телефони, дати, імена).
- Підключіть, при можливості, систему підтвердження авторизації через телефон.
- Активуйте систему оповіщень, у випадку авторизації у ваш акаунт із невідомого пристрою.
- Не використовуйте суміжні (Об’єднані) акауни.

Якщо користувач буде дотримуватись усіх перерахованих правил, то він зможе значно підвищити рівень надійності своєї електронної скриньки.

Висновок. Отже, електронна пошта є дуже легким та корисним методом обміну даними, але вона має досить серйозні проблеми із безпекою. Багато хакерів можуть використати ці проблеми для здобуття ваших персональних даних, використовуючи для цього віруси, спам-повідомлення, або ваші власні авторизаційні дані. Для повноцінного захисту, користувач має одночасно користуватися надійними сервісами електронних скриньок, і дотримуватись певних правил, щоб компенсувати недоліки автоматичної системи безпеки.