ПРЕВЕНТИВНІ АНТИСПАМ ЗАХОДИ

Райта Діана Анатоліївна
Львівський державний університет безпеки життєдіяльності
Кухарська Н. П., к. ф.-м. н., доцент

Сотні мільйонів людей у всьому світі для формальної та неформальної комунікації використовують електронну пошту. Більшість з них хоча б один раз за час користування стикалась з проблемою засмічення поштової скриньки “небажаними повідомленнями” (спамом). Так, у 2016 році, за даними Cisco Systems, на спам припало майже дві третини (65%) повідомлень усієї електронної пошти, з них 10% розглядалися як небезпечні [1].

Спам – це масова розсилка різного змісту повідомлень користувачам, які не виявляли бажання їх отримувати.

Більшість спам-розсилок мають рекламний, комерційний характер. Так, у 2016 році в поштовому трафіку часто зустрічалися повідомлення від фабрик і заводів, розташованих на території Китаю, які містили рекламу виробленої ними продукції [2]. У Китаї соціальні мережі в основному внутрішні, світові гіганти на кшталт Facebook заборонені. Прагнучи вийти на міжнародний ринок, китайські підприємці, володіючи меншою кількістю доступних легальних засобів, для реклами продукції активно використовують електронну пошту. Яку шкоду завдають подібні спам-розсилки? По-перше, вони засмічують поштові скриньки, по-друге, змушують користувачів витрачати гроші на оплату надлишкового трафіку, а також свій час на видалення цього непотребу.

Останнім часом спостерігається тенденція до збільшення частки спаму іншого різновиду – листів зі небезпечними вкладеннями. Як правило, вони містять даунлоадери – шкідливі програми сімейства Trojan. Щоб змусити користувача перейти за шкідливим посиланням чи відкрити вкладення, зловмисники використовують методи соціальної інженерії. Зараз спамери не переслідують ціль здивувати чи залякати користувача. Вони намагаються надати повсякденного вигляду електронному листу, зробити його таким, щоб він не відрізнявся від решти кореспонденції. Очевидно, ними враховується той факт, що

значна частина теперішніх користувачів мережі Інтернет освоїла ази інформаційної безпеки і може відрізнити реальну загрозу від фальшивої. Користувача спонукують відкрити небезпечне вкладення, маскуючи його під рахунки від різних організацій, квитанції, квитки, скани документів, голосові повідомлення, повідомлення від магазинів тощо. Деякі такі листи не містять тексту взагалі.

Також спостерігається збільшення з року в рік кількості шахрайських атак, спрямованих на клієнтів фінансових організацій. Шахраї вигадують все більш вишукані схеми обману, застосовують фішинг. Спамери намагаються виманити в отримувача листа номери його кредитних карток чи паролі доступу до систем онлайнових платежів. Фішинговий спам-лист, як правило, маскують під офіційне повідомлення від адміністрації банку. У ньому йдеться про те, що одержувач повинен підтвердити відомості про себе, інакше його рахунок буде заблокований, і вказується адреса підставного сайту, де знаходиться форма, яку треба заповнити. Серед даних, що потрібно повідомити, є і ті, що цікавлять шахраїв. Жертві не просто здогадатися, що її обманюють, дизайн підробленого сайту імітує дизайн офіційного сайту банку. До речі, у 2016 році з фішингом зіткнулися 15,29 % унікальних користувачів електронної пошти [2].

Потік спаму можна мінімізувати, якщо дотримуватимуться певних правил. Сформулюємо їх.

- Не слід публікувати електронну адресу на загальнодоступних сайтах у відкритій формі. Необхідно використовувати спеціальні символи або JavaScript для її кодування. Також можна подавати адресу у вигляді зображення. Це ускладнить процес її розпізнавання програмами збору адрес.
- Перш ніж зареєструватися на якому-небудь із сервісів, варто пересвідчитися, чи не даєте згоду на отримання розсилок, натискаючи на кнопку “Зареєструватися”.
- Більшість власників електронних скриньок мають акаунти в соціальних мережах. Останнім часом на різних сайтах доволі часто пропонується авторизуватися через соціальні мережі. З метою зменшення кількості спаму

рекомендуємо скористатися наданою можливістю.

- Не варто вказувати під час реєстрації на маловідомих форумах і сайтах адресу поштової скриньки, що використовується для особистого та ділового листування. Для цих цілей можна створити іншу поштову скриньку, або можна скористатися послугами відповідних служб для отримання одноразової E-mail адреси, наприклад, сервісу – http://mailinator.com/.
- Ні в якому випадку не слід відповідати на спам або переходити за посиланнями, вказаними у листі, в тому числі за такими, що забезпечують відмову від розсилки. Такі дії дадуть знати спамерам, що адреса діюча і кореспонденція читається власником скриньки. Також не слід відкривати вкладення.
- Щоб не відстежувалася активність користувача, бажано відключити завантаження графіки, що міститься в листах.
- Рекомендуємо відмовлятися від переходу за посиланнями, навіть такими, що отримані з адреси, яка є у переліку контактів, якщо таке посилання викликає підозру.
- У поштовій скриньці слід налаштувати антиспам-фільтр таким чином, щоб він не пропускав листи, в яких у полях ”Кому” і ”Копія” не фігурує ваша адреса.
- Якщо у поштовій скриньці все ж таки виявся лист, що містить спам, то його слід позначити, натиснувши відповідну кнопку. Чим більше листів із спамом буде помічено, тим точніше працюватимуть фільтри.

ЛІТЕРАТУРА

1. Email Spam Surged in 2016: 65% of Emails are Spam [Electronic resource] // HIPAA Journal. – Access mode : https://www.hipaajournal.com/email-spam-surged-2016-65-emails-spam-8676/
2. Kaspersky Security Bulletin. Спам и фишинг в 2016 году [Электронный ресурс] / Д. Гудкова, М. Вергелис, Н. Демидова, Т. Щербакова. – Режим доступа : https://securelist.ru/kaspersky-security-bulletin-spam-and-phishing-in-2016/30205/