CERT-UA

Рекомендації
13 серпня 2015

CUA-15-05R
БЕЗПЕКА ПОШТОВОГО СЕРВІСУ

Автор: Іван Соколов
Державна служба спеціального зв'язку та захисту інформації України
Державний центр кіберзахисту та протидії кіберзагрозам
04119, Україна, м. Київ, вул. Мельникова, 83б
тел.: +380 44 281 88 25
факс: +380 44 489 31 33
www: cert.gov.ua

ЗМІСТ

1. Загальна інформація про публічний електронний поштовий сервіс

Багато сервіс-провайдерів надають безкоштовні електронні поштові акаунти (наприклад, Gmail, Yahoo!). Зазвичай, доступ до цих сервісів можливий за допомогою веб-браузерів (наприклад, Firefox, Chrome). Такий спосіб має переваги:

- можливість читати пошту з будь-якого комп'ютера (оскільки маже скрізь є браузер),
- можливість отримати та використовувати великі об'єми простору для зберігання даних,
- фільтрація спаму, антивірусний захист, автоматичні дії з поштою тощо.

Якість цих послуг зазвичай досить висока, а користуватись ними — легко, оскільки сервіс-провайдер налаштовує їх та Вам надається зручний і зрозумілий інтерфейс користувача. Прикладом корисного (але не дуже безпечного!) варіанту використання публічних поштових сервісів може бути організація пересилання пошти з безкоштовного поштового акаунту на основний з попередньою фільтрацією спаму.

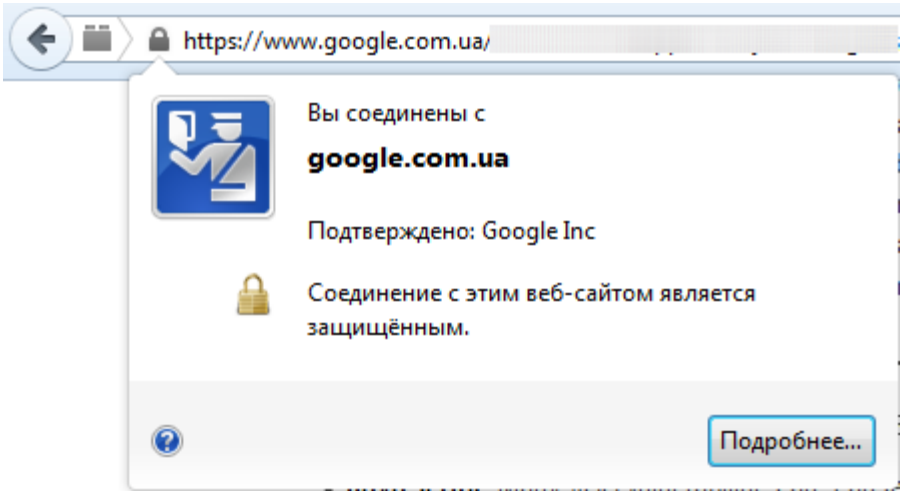
2. Ризики, пов'язані з використанням публічних електронних поштових сервісів

2.1 Безкоштовні електронні поштові сервіси не гарантують надійного захисту від різних загроз

Оскільки Ви не сплачуєте за користування акаунтом, сервіс-провайдер не зацікавлений безпосередньо у тому, щоб надати користувачеві максимально якісний сервіс. Часто сервіс-провайдер не робить це свідомо, мотивуючи користувача перейти на платний і більш захищений сервіс. Загальне правило “безкоштовний сир — тільки у мишоловці” діє і тут і, не заключаючи відповідний договір з сервіс-провайдером, Ви отримуєте сервіс “як є”, тобто без можливості скаржитись. Крім того, коли сервіс-провайдер не отримує коштів від користувача, підвищується ризик того, що він спробує отримати кошти у результаті продажу інформації про користувачів. Тому, доцільно уважно переглядати умови користування цим сервісом.

2.2 Користування акаунтом може бути не достатньо конфіденційним

Цей ризик виникає, коли поштові повідомлення відправляються та приймаються у відкритому вигляді (так званий, формат plaintext), відповідно, можуть бути легко перехоплені. Якщо сервіс-провайдер надає послугу шифрування, рекомендується використовувати її. Прикладом розуміння цього ризику був перехід багатьох відомих у світі поштових публічних сервісів на обов'язкову підтримку протоколу SSL. При цьому, в рядку адреси повинно бути вказано “https:” замість “http:”. Для того, щоб увімкнути режим підтримки цього протоколу, достатньо пошукати “захищений режим” у налаштуваннях браузеру. Приклад того, як захищене протоколом SSL-з'єднання виглядає при входженні на сервіс google, наведено нижче:



2.3 Використання безкоштовних публічних електронних поштових сервісів може суперечити політиці безпеки

Якщо Ви плануєте користуватись у службових цілях безкоштовними електронними публічними сервісами, узгодьте це з Вашим працедавцем. Це дозволить уникнути суперечок з корпоративною політикою інформаційної безпеки.

Для державних потреб не рекомендується користуватись публічними поштовими сервісами, оскільки це часто призводить до витоку службової інформації. За результатом опитування CERT-UA 134 державних установ у 2015 році з'ясовано, що тільки 16 з них мають власний поштовий сервіс.

2.4. Ризик втрати доступності

Деякі сервіс-провайдери залишають за собою право видалити усі дані користувача у разі тривалого не користування сервісом певним користувачем. Щоб уникнути цього, треба уважно читати умови надання сервісу, які надаються сервіс-провайдером. Також, доцільно поцікавитись щодо часу доби, у який відбувається обслуговування поштових серверів, щоб це не заважало працювати з електронною поштою. Особливо актуально це у випадку, коли сервіс-провайдер працює у іншому часовому поясі.

3. Загрози поштового сервісу, та рекомендації для їх уникнення

3.1 Спам

Зі спамом не тільки пов'язана необхідність читати небажану пошту, а й ризик отримання пошти з додатком, який містить віруси. Спам — постійний супутник власників електронної пошти, якого не можливо уникнути але можливо мінімізувати, для цього необхідно виконувати наступні рекомендації:

- **добре обдумуйте публікацію Вашої електронної поштової скриньки** — кожна відповідь на поштове повідомлення, кожен пост Вашої адреси електронної поштової скриньки у мережі Інтернет, озвучення або написання на папері — можуть бути використані спамерами для розсилання спаму. Спамери можуть автоматизовано збирати та використовувати залишені у мережі Інтернет. Щоб замаскувати свою адресу від спамерів, використовуйте заміну для символів "@" та ".", наприклад:

  cert@cert.gov.ua => cert at cert dot gov dot ua

- **ознайомтесь з політикою приватності** — перед використанням електронної поштової скриньки у мережі Інтернет на багатьох веб-сайтах доцільно прочитати політику розповсюдження персональних даних, щоб розуміти що далі може статись з введеними даними.
- **будьте обережні з налаштуваннями за замовчанням** — у ході реєстрації акаунту (підписання на сервіс), може бути опція щодо згоди на отримання електронної пошти щодо інших продуктів та сервісів. Часто без відключення цих опцій користуватись таким сервісом стає неможливим (нав'язлива реклама).
- **використовуйте фільтри або відмічайте спам** — багато поштових клієнтів мають функціонал для забезпечення функцій блокування електронних адрес або налаштування отримання пошти тільки з поштових адрес, які знаходяться у списку контактів. Боротьба зі спамом набагато ефективніша при поєднанні відмічання спаму з фільтрацією. Відмічайте спам — якщо сервіс-провайдер надає такий функціонал, відмічання пошти, як спам, автоматично навчає антиспам-фільтр поштового сервісу і він починає краще боротись зі спамом і той навіть не потрапляє до Вашої поштової скриньки у подальшому.
- **не переходьте по посиланням у спамі** — іноді перехід по посиланню у спамі призводить до автоматичного підтвердження того, що Ваша електронна поштова скринька активна. Небажані електронні повідомлення також часто мають опцію щодо відписання від їх отримання, а коли користувач обирає цю опцію — це також дозволяє зібрати інформацію про активність Вашої скриньки.
- **вимкніть автоматичне завантаження графіки та HTML у пошті** — багато спамерів використовують HTML з приєднаними графічними даними, які відстежують хто відкрив електронне поштове повідомлення. Коли Ваш поштовий клієнт

завантажує графіку з веб-серверу, спамер дізнається що Ви отримали повідомлення.

- **використовуйте налаштування безпеки у соціальних мережах** — сайти соціальних мереж зазвичай дають можливість обирати хто має доступ до перегляду Вашої адреси поштової скриньки. Вирішіть, сховати або показати його маленькій групі осіб, яким Ви довіряєте. Пам'ятайте, що коли використовуєте функціонал на цих сайтах, можете надати їм доступ до Ваших персональних даних. Таким чином, будьте уважні стосовно функціоналу, який використовуєте.
- **не спамте інших користувачів** — будьте відповідальним користувачем. Іноді необдумане перенаправлення пошти іншим контактам з Вашої книги контактів може призвести до отримання ними небажаної пошти.

3.2 Небезпечні додатки

Додатки до електронних документів (e-mail attachments) — не тільки зручний спосіб обмінюватись файлами, а ще й джерело отримання вірусів. Будьте дуже обережні та уважні при відкритті додатків.
Особливості електронної пошти та загрози, пов'язані з нею:

- **Електронна пошта легко циркулює** — вірус, який заразив комп'ютер, може швидко знайти усі наявні електронні поштові адреси та самостійно інфікувати усіх адресатів, надіславши поштове повідомлення, яке містить вірус, усім хто є у адресній книзі. Зловмисники часто користуються довірою користувачів до адресатів, які є у адресній книзі і це часто призводить до вірусних епідемій.
- **Поштові програми мають широкий функціонал** — майже будь-який файл може бути прикріпленим до електронного поштового повідомлення, таким чином це дає свободу зловмиснику у виборі типу вірусу, який може бути надісланий. Крім того, поштові програми можуть автоматично завантажувати додатки до електронних листів, які негайно компрометують комп'ютер вірусами, які містяться всередині.

Кроки, які рекомендується зробити користувачу електронної пошти для захисту адресної книги

- **будьте обережні при відкритті атачментів, навіть від відомих Вам людей** — навіть якщо електронний лист виглядає, як лист від Вашого рідного, це може бути не так. Завданням зловмисника є ввести в оману користувача, щоб він відкрив атачмент. Багато вірусів можуть підміняти (англ. - to spoof) адресу відправника, роблячи так, щоб електронний лист виглядав як відправлений кимось іншим. Якщо можливо, перевірте чи відправляв Вам електронний лист відправник перед тим, як відкривати атачменти. Це ж стосується листів від Вашого Інтернет-провайдера або розробника програмного забезпечення, банку та антивірусу, послугами яких Ви користуєтесь тощо. Крім того, виробники програмного забезпечення та антивірусів не висилають програмне забезпечення за допомогою

електронної пошти. Приклади інцидентів, пов'язаних з цим видом загрози наведено у публікаціях CERT-UA (http://cert.gov.ua/?p=429, http://cert.gov.ua/?p=2109, http://cert.gov.ua/?p=2128).

- **оновлюйте програмне забезпечення** — інсталюйте патчі, таким чином зловмисник не зможе отримати у своє розпорядження відомі вразливості (більш детально про патчі написано у US-CERT — тут). Багато операційних систем надають можливості автоматичного оновлення. Якщо ця опція доступна — користуйтесь нею.
- **довіряйте інстинктам** — якщо електронне поштове повідомлення або атачмент здаються Вам підозрілими, не відкривайте їх, навіть якщо антивірус повідомляє, що повідомлення чисте. Зловмисники можуть постійно випускати нові віруси, таким чином антивірусне програмне забезпечення не виявляє їх оскільки не має відповідної сигнатури у своїх базах оновлень. У крайньому випадку, зв'яжіться з особою, яка вислала Вам повідомлення та дізнайтесь про деталі листа, який вона Вам відправила та атачменти. Це важливо, особливо для перенаправленої пошти (від англ. - forwarded), оскільки навіть відправлені від легітимного відправника поштові повідомлення можуть містити віруси.
- **збережіть та проскануйте антивірусом атачмент перед відкриттям —** перевірте чи оновлено антивірусні бази (більш детально про антивіруси у US-CERT написано тут), збережіть атачмент на диск, вручну проскануйте антивірусом атачмент на диску і якщо атачмент чистий — відкривайте його.
- вимкніть опцію автоматичного завантаження атачментів — для спрощення процесу читання електронної пошти, багато поштових програм мають увімкнену за замовчанням опцію автоматичного завантаження атачментів. Перевірте, що ця опція вимкнена у Вашому програмному забезпеченні.
- Використовуйте різні облікові записи для читання електронної пошти на комп'ютері — більшість операційних систем мають можливості створити облікові записи з різними повноваженнями. Вирішіть використовувати для читання пошти обліковий запис у операційній системі, який має обмежені повноваження. Деякі віруси потребують адміністративних привілеїв для інфікування комп'ютера.
- Впроваджуйте додаткові практики з безпеки — можливо фільтрувати деякі види атачментів за допомогою поштового програмного забезпечення або фаєрволів (більш детально про антивіруси у US-CERT написано тут).
- **в разі підтримки протоколу PGP використовуйте його для вхідної чи вихідної електронної пошти** - **PGP** (англ. *Pretty Good Privacy*) — комп'ютерна програма, також бібліотека функцій, що дозволяє виконувати операції шифрування і цифрового підпису повідомлень, файлів та іншої інформації, поданої в електронному вигляді, у тому числі прозоре шифрування даних на запам'ятовуючих пристроях, наприклад на твердому диску.
- **в разі підтримки двофакторної авторизації використовуйте її** - основною її відмінністю від звичайної авторизації є додаткове введення секретного коду, який висилається користувачу у вигляді смс повідомлення або формується додатком (на iPhone, BlackBerry або Android).

Зміни до документу

- 13.08.2015: Перший випуск.