Рекомендації з підвищення рівня безпеки комп'ютерів для користувачів

1. Не запускати виконувані файли (формати adp, .apk, appx, appxbundle, bat, cab, chm, cmd, com, cpl, dll, dmg, exe, hta, ins, isp, iso, jar, js, jse, lib, lnk, mde, msc, msi, msix, msixbundle, msp, mst, nsh, pif, ps1, scr, sct, shb, sys, vb, vbe, vbs, vxd, wsc, wsf, wsh), а також не розпаковувати таких файлів архіваторами.

2. Не запускати в інформаційній системі з правами адміністратора програм cmd та powershell та будь-яких скриптів (* script.exe).

3. Не зберігати автентифікаційних (облікових) даних у відкритому доступі (наприклад, на робочому столі). Використовувати для зберігання паролів паперові носії або спеціальні програмні засоби.

4. Не використовувати службову електронну скриньку для особистої переписки та навпаки, а її реквізити для реєстрації на загальнодоступних сервісах мережі Інтернет (п.4 Постанови КМ України № 522 від 2002 року «Про затвердження Порядку підключення до глобальних мереж передачі даних», п. 2 Постанови КМ України № 851 від 2015 року «Про деякі питання використання доменних імен державними органами в українському сегменті Інтернету»).

5. Забезпечувати перевірку всієї вхідної електронної кореспонденції. Приділяти увагу несподівано отриманим електронним листам, особливо від незнайомих поштових адрес. Використовувати додаткові засоби комунікації з метою перевірки відправника листа (наприклад у телефонному режимі). Звертати особливу увагу та не відкривати одразу електронні листи з ознаками терміновості його відкриття або особливої важливості (використовується для створення тиску на користувача та забезпечення відкриття листа з вкладенням без перевірочних заходів), тематичними відмінностями (тема листа відмінна від функціональної діяльності), а також уважно перевіряти відомості, що наведені у його тексті (наприклад, вони застарілі та не актуальні на поточний момент). У разі виявлення таких листів необхідно проінформувати адміністратора безпеки та співробітника Управління СБУ.

6. Забезпечити перевірку відправника кожного листа, провести його верифікацію. Для цього необхідно порівняти дані наведені у полях "від кого:" заголовка листа та у "Return-Path:" з технологічної інформації про електронний лист. Відмінність даних свідчить про підміну адресата, тому відкривати лист забороняється. У такому випадку повідомте адміністратора безпеки, а також співробітника Управління СБУ, для отримання подальших інструкцій.

7. Перед відкриттям вкладення до електронного листа необхідно встановити його розширення (може бути приховано або змінено), перевірити його антивірусним програмним засобом.

8. Не переходити за невідомими посиланнями (URL), які вкладено в електронний лист. Перевірити їх реалістичність шляхом наведення на них курсору миші та визначення ресурсу на який насправді буде переадресовано за посиланням. Перевіряйте ресурси з використанням яких Вам пропонують авторизуватися (наприклад, facebook не пропонуватиме вам авторизуватися через twitter або навпаки). У разі підміни або підозри щодо спроби підміни повідомте адміністратора безпеки, а також співробітника Управління СБУ.

9. Введення автентифікаційних даних здійснювати лише на веб-ресурсах, що використовують захищене з'єднання HTTPS. Провести попередню перевірку SSL-сертифікату веб-сайту (зелений замочок в лівому куті адресного рядка), та встановити, що він не клонований або не підроблений, а також відноситься до власника ресурсу. У разі відмінності власника сертифіката від веб-ресурсу, який ви відвідуєте – вводити на ньому свої персональні або облікові дані заборонено.