Прим. № 1

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки

вул. Володимирська, 33, м. Київ, 01601
Тел. (044) 256-91-64, E-mail: dkib@ssu.gov.ua
Код ЄДРПОУ 00034074

21.09.21 № 30/4/Р-25-П/16/10191

Артему РУМЯНЦЕВУ

Щодо надання публічної інформації

За дорученням керівництва Служби безпеки України Департаментом опрацьовано Ваш запит щодо рекомендацій у сфері кібербезпеки.

За результатами опрацювання повідомляємо, що на офіційному сайті СБ України (https://ssu.gov.ua/yak-podbaty-pro-kiberbezpeku) оприлюднено необхідну Вам інформацію.

«Безпека електронних пристроїв:

1. Регулярно оновлюйте системи захисту ваших пристроїв.
2. Систематично робіть резервне копіювання важливих файлів.
3. Встановіть режим конфіденційності та безпеки для вебсайтів.
4. Під час оплати в інтернеті звертайте увагу на електронну адресу: «https://» - це означає, що сайт вживає додаткові заходи для безпеки своїх клієнтів; «http://» - посилання не є безпечним.
5. Не використовуйте службові електронні скриньки для приватного листування.
6. Скануйте перед підключенням USB та інші зовнішні пристрої на наявність шкідливих додатків і вірусів.

Безпечне підключення до Wi-Fi

Безкоштовне підключення до Wi-Fi у публічних місцях часто відбувається без введення паролів. Це робить ваш пристрій вразливим для зламу.

1. Під час входу до мережі Wi-Fi використовуйте лише ті точки доступу до Wi-Fi, які мають протоколи безпеки для захисту бездротового з'єднання WPA чи WPA-2.
2. Оптимальний варіант – користуватись особистим Wi-Fi модемом або здійснювати вхід в Інтернет за передплаченим пакетом послуг мобільного оператора.
3. Вимикайте функцію «Автоматичного підключення до Wi-Fi».

Захист смартфону від програм-шпигунів

Більшість шпигунських програм «вшиваються» саме в мобільні додатки. Коли ви встановлюєте їх на смартфон, то власноруч дозволяєте зчитати вашу геолокацію, список контактів, акаунти у соцмережах та поштові скриньки.

1. Встановлюйте додатки лише з офіційних та перевірених сервісів: Chrome Store, Add-ons та Play Market для Android, App Store для OS.

2. Не дозволяйте операційній системі смартфона (планшета, ПЕОМ) автоматично встановлювати додатки з невідомих джерел.

3. Періодично видаляйте додатки, якими не користуєтеся.

Безпека електронного листування

Якщо зловмисники «зламають» вашу електронну пошту, вони можуть спробувати змінити паролі, отримати доступ до особистих фотографій та відео, розсилати спам від вашого імені.

1. Увімкніть двофакторну автентифікацію за допомогою мобільного пристрою. Якщо стороння особо спробує отримати пароль до вашої поштової скриньки, ви автоматично отримаєте SMS-повідомлення про несанкціонований вхід.

2. Встановіть надійний пароль і не використовуйте для його відновлення російські сервіси «Yandex.ru», «Mail.ru».

Не відкривайте на пристроях вкладення підозрілих листів, що мають такі розширення як «.exe», «.bat», «.cmd», «.vbs», «.docm», «.xlsm» тощо.

Перший заступник
начальника Департаменту **Олександр РОСПУТЬКО**