ПЕРШОЧЕРГОВІ КРОКИ ПРИ ВИЯВЛЕННІ КІБЕРАТАКИ АБО КІБЕРІНЦИДЕНТУ ТА ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УВАГА!

При виявленні кібератаки або кіберінциденту необхідно:

1) Невідкладно (не пізніше 30 хвилин) з моменту виявлення, інформувати Національний координаційний центр кібербезпеки на report@ncscc.gov.ua про виявлену кібератаку або кіберінцидент, що потенційно може мати критичні наслідки для кібербезпеки держави із зазначенням об'єкта кібератаки (кіберінциденту), часу її здійснення та іншої наявної інформації.
2) Невідкладно повідомити Урядову команду реагування на кіберінциденти про виявлену кібератаку або кіберінцидент на https://cert.gov.ua/ (тел. +38 (044) 281-88-25)
3) Протягом 12 годин після виявлення такої кібератаки/кіберінцидента у встановленому порядку надавати Національному координаційному центру технічну інформацію (індикатори компрометації, тип атаки, особливості механізму реалізації тощо), а також інформацію щодо можливого джерела, потенційних наслідків, додаткових обставин, вжитих та запланованих заходів реагування.
4) При підозрі у виявленні кібератаки або кіберінциденту, повідомте Департамент Кіберполіції за тел.: 0800-505-170, після з'єднання: 10-86; 047-252-0926; 063-634-1357, або за формою https://ticket.cyberpolice.gov.ua/

ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Зберігання та передача даних

Недотримання окремих правил безпеки під час здійснення службових обов’язків працівниками органів виконавчої влади та місцевого самоврядування, посадовими особами державних підприємств, установ, організацій може призвести до втрати чи крадіжки мобільних телефонів, персональних ноутбуків, магнітних носіїв інформації тощо. Вказане ставить під загрозу збереження персональних даних та може призвести до розголошення інформації з обмеженим доступом.

Сприятливі умови для реалізації кіберзагроз виникають через порушення базових вимог законодавства про захист інформації в

інформаційно-телекомунікаційних системах *(далі - ІТС),* а також внаслідок таких чинників:

• *здійснення несанкціонованого доступу до баз даних;*

• *копіювання та передача через незахищений канал мережі Інтернет документальних матеріалів, що містять службову інформацію;*

• *використання особистих технічних засобів у складі виробничих автоматизованих систем (USB-флеш накопичувані);*

• *підключення до комп'ютерних систем технічних засобів із модулями передачі даних (Bluetooth, GSM тощо), призначених для створення каналів зв'язку з мережами загального користування та іншими електронними пристроями;*

• *незахищеність ІТС за допомогою актуальних версій антивірусного програмного забезпечення.*

З метою уникнення негативних наслідків у випадку втрати або викрадення носіїв інформації необхідно:

• *блокувати пристрої щоразу після закінчення роботи з ними*

• *встановити паролі на усі пристрої, що перебувають у користуванні, а також паролі/коди на доступ до всіх облікових записів;*

• *систематично здійснювати резервне копіювання важливих файлів на окремі фізичні носії та забезпечувати надійне зберігання таких носіїв;*

2. Соціальні мережі

З метою уникнення несанкціонованого доступу до персональних акаунтів, зареєстрованих у соціально-орієнтованих ресурсах мережі Інтернет, необхідно:

• *встановити надійний пароль для входу в обліковий запис. При цьому рівень захищеності акаунта та інформації, яка в ньому міститься, залежить від складності встановленого паролю;*

• *використовувати функцію подвійної авторизації. Щоб увійти до профілю з незнайомого пристрою, сервіс вимагатиме пройти додаткову ідентифікацію як власника акаунта. При цьому на вказаний номер телефону чи на поштову скриньку буде надіслано повідомлення з кодом підтвердження або необхідно буде ввести один із паролів, які попередньо були збережені через інший обраний спосіб підтвердження;*

• *здійснити додаткові налаштування профілю в соціальних мережах з метою отримання інформації щодо несанкціонованого доступу до ресурсів з невідомого пристрою або Інтернет-браузера;*

• *при створенні акаунтів у соціальних мережах використовувати у якості логіна поштову адресу надійного сервісу (наприклад «Google», «Yahoo»), або українських поштових сервісів. Не рекомендується користуватися російськими сервісами;*

• ***не здійснювати*** *авторизацію особистих чи робочих, корпоративних профілів з незнайомих чи незахищених пристроїв. Існує ймовірність, що після завершення роботи не буде здійснено вихід із облікового запису або пристрій*

запам'ятає вказаний при вході логін та пароль. Крім того, існує ймовірність ураження такого пристрою шкідливим програмним забезпеченням, що може здійснювати збір та передачу відомостей щодо паролів та логінів зацікавленим особам;

• ***не відкривати*** *вкладень у підозрілих повідомленнях від адресатів щодо яких виникають сумніви;*

• ***пам'ятайте,*** *що саме фітинг (довідково:* ***фішинг*** *- вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі Інтернет персональних даних клієнтів, сервісів із переказу або обміну валюти, Інтернет-магазинів) є найпоширенішим способом отримання зловмисниками паролів до поштових скриньок та сторінок у соціальних мережах.*

Також слід враховувати, що у ході гібридної агресії з боку РФ соціальні мережі активно використовуються для збору додаткових відомостей щодо місць регулярного перебування особи, її родичів, колег, особистих уподобань та іншої приватної інформації.

З метою недопущення отримання зацікавленими особами додаткової (приватної) інформації стосовно особи, членів її сім'ї, колег рекомендується:

• ***не публікувати*** *у соціальних мережах інформацію, що може поставити під загрозу особисте життя особи, життя членів її сім'ї та інших осіб;*

• *членам сімей військовослужбовців не публікувати фото- та відеоматеріали, за допомогою яких можна визначити їх місцезнаходження, отримати дані про озброєння та діяльність військової частини, окремих збройних військових формувань, що беруть участь у проведенні операції об'єднаних сил на сході України. Вказані дії можуть загрожувати життю та здоров ю людей, а також створює передумови до вербувальної діяльності спеціальних служб іноземних держав, насамперед Російської Федерації;*

• *обмежити доступ до приватної інформації в налаштуваннях конфіденційності соціальної мережі. Вибрати налаштування, які найбільше захищають додаткові відомості про власника акаунта. Зокрема, не зазначати геолокацію (місце розташування);*

• *періодично переглядати список «друзів» у соціальній мережі. Якщо серед них є незнайомі або підозрілі акаунти, необхідно їх видалити, оскільки статус «друга» відкриває доступ до більшого обсягу приватної інформації про особу. У подальшому необхідно бути уважними під час додавання до списку «друзів» нових користувачів;*

• ***не використовувати*** *російські соціальні мережі «ВКонтакте» та «Одноклассники», а також російські пошукові системи «Mail.ru» та «Yandex» (у т.ч. із застосуванням сервісів VPN), доступ до яких обмежено відповідно до Указу Президента України № 184/2020, оскільки відповідно до федеральних законів РФ власники вказаних ресурсів можуть передавати російським спецслужбам відомості щодо персональних даних користувачів акаунтів (e-mail, номер мобільного телефону, дата та IP-адреса реєстрації,*

дата та IP-адреса останнього відвідування тощо).

Слід зазначити, що за розповсюдження через соцмережі матеріалів із закликами до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України, передбачена кримінальна відповідальність.

Також слід звернути увагу на те, що окремі публікації, розміщені посадовими особами органів виконавчої влади на їх персональних сторінках у соціальних мережах, можуть слугувати інформаційним приводом, який у подальшому буде використаний для підриву авторитету державної влади в цілому, штучного загострення суспільно-політичної ситуації в державі та здійснення інших деструктивних дій на шкоду державним інтересам України.

3. Використання додатків до смартфонів

Під час встановлення тих чи інших додатків на власний телефон ці програмні продукти можуть вимагати доступу до певної інформації на використовуваному пристрої, насамперед геолокації, списку контактів, акаунтів у соціальних мережах та поштових скриньок.

За наявними даними, більшість шпигунських програм «вшиваються» саме в мобільні додатки, які цікавлять конкретну аудиторію. Тому необхідно бути уважним під час встановлення додатків, особливо якщо робити це з невідомих та неперевірених сервісів.

З метою унеможливлення завантаження на особистий пристрій програм-шпигунів необхідно дотримуватись таких правил:

• *встановлювати додатки лише з офіційних та перевірених сервісів (Chrome Store, Google Play Store для Android, App Store для iOS);*

• ***заборонити*** *операційній системі смартфона (планшета, ПЕОМ) автоматично встановлювати додатки з невідомих джерел, шляхом здійснення відповідних налаштувань пристрою;*

• *періодично здійснювати видалення усіх особистих пристроїв від додатків, які не використовуються.*

4. Електронне листування

Щоб уникнути зламу електронної поштової скриньки, необхідно:

•*увімкнути двофакторну автентифікацію за допомогою мобільного пристрою. В такому випадку під час спроби отримання паролю до поштової скриньки сторонніми особами буде надходити попередження на мобільний телефон у вигляді SMS-повідомлення про спробу злому;*

• *встановити надійний пароль;*

• *не використовувати для відновлення паролю російські сервіси («Yandex.ru», «Mail.ru» тощо);*

• *не запускати на пристроях вкладення підозрілих листів, що містять виконуваний файл з такими розширеннями як «.exe», «.bat», «.cmd», «.vbs»,*

«.docm», «.xlsm» тощо;

• державні службовці повинні пам'ятати, що службові електронні скриньки не слід використовувати для приватного листування.

5. Доступ до мережі Інтернет

Одним із найпоширеніших способів доступу до мережі Інтернет у публічних місцях є підключення до відкритих точок Wi-Fi. Зазвичай вони є безплатними та доступ до них здійснюється без введення паролів. Саме відсутність паролю робить їх вразливішими для злому з боку зацікавлених осіб, які мають на меті отримати персональні дані та відомості, що зберігаються на телефоні, планшеті, ПЕОМ тощо.

Щоб уникнути перехоплення даних сторонніми особами, необхідно:

•під час здійснення доступу до мережі використовувати лише ті точки Wi-Fi, які мають протоколи безпеки для захисту безпровідного з'єднання WPA чи WPA-2;

•у публічних місцях найкраще користуватись особистим Wi-Fi модемом або здійснювати доступ до мережі Інтернет з мобільного пристрою за передплаченим пакетом послуг мобільного оператора;

•на FIEOM, мобільних пристроях та планшетах необхідно вимкнути функцію «Автоматичне підключення до Wi-Fi».