На допомогу дорослим)))

Характеристика ключових факторів ризику

1. Зберігання та передача даних

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

- встановити паролі на усі пристрої, що перебувають у користуванні (PIM-коди, паролі на вхід до всіх облікових записів, паролі на планшетах та ноутбуках тощо);
- систематично робити резервне копіювання важливих файлів;
- блокувати пристрої щоразу після закінчення роботи з ними.

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 акаунту та інформації, що знаходиться у ньому, залежить від складності установленого паролю:
- використовувати функцію подвійної авторизації. Щоб увійти до профілю з незнайомого пристрою, сервіс вимагатиме пройти додаткову ідентифікацію як власника акаунту. При цьому на вказаний номер телефону або 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 несанкціонованих входів 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, доступ до яких заборонено в Україні, оскільки через персональну електронну скриньку можна отримати пароль, а відтак доступ до профілів, зареєстрованих у соціальних мережах;
- не здійснювати авторизацію особистих чи робочих, корпоративних профілів з незнайомих чи незахищених пристроїв. Існує ймовірність, що після завершення роботи не буде здійснено вихід із свого 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;
- пам'ятайте, що саме фітинг (довідково: фітинг - 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.
- періодично переглядати список друзів у соціальній мережі. Якщо серед них є незнайомі або підозрілі люди (акаунти), необхідно їх видалити, оскільки статус «друга» відкриває доступ до більшого обсягу приватної інформації про особу. В подальшому необхідно бути уважними під час додавання до списку «друзів» нових користувачів.
- не рекомендується використовувати російські соціальні мережі «ВКонтакте» та «Одноклассники», доступ до яких заборонено, оскільки останні на вимогу спецслужб РФ

можуть передавати відомості щодо персональних даних власників акаунтів (e-mail, номер мобільного телефону, дата та IP-адреса реєстрації, дата та IP-адреса останнього відвідування тощо).

3. Використання додатків до смартфонів

3 метою унеможливлений завантаження на особистий пристрій програм- шпигунів необхідно дотримуватись таких правил:

- встановлювати додатки лише з офіційних та перевірених сервісів (Chrome Store, Addons та Play Market для Android, App Store для OS);
- заборонити операційній системі смартфоиа (планшета, ПЕОМ) автоматично встановлювати додатки з невідомих джерел шляхом здійснення відповідних налаштувань пристрою;
- періодично здійснювати чистку 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 («Yqndex.ru», «Mail.ru» тощо);
- не запускати на пристроях вкладення підозрілих листів, що містять виконуваний файл з такими розширеннями як «.exe», «.hat», «.cmd», «.vhs», «.docm», «.xlsm» тощо;
- державні службовці та військовослужбовці повинні пам 'ятати, що службові електронні скриньки не слід використовувати для приватного листування.

5. Вихід до мережі Інтернет

Щоб уникнути перехоплення даних сторонніми особами, необхідно:

- під час здійснення входу до мережі використовувати лише ті точки доступу до WiFi, які мають протоколи безпеки для захисту бездротового з'єднання WPA чи WPA-2;
- у публічних місцях найкраще користуватись особистим Wi-Fi модемом або здійснювати вхід бо мережі Інтернет з мобільного пристрою за передплаченим пакетом послуг мобільного оператора;
- на ПЕОМ, мобільних пристроях та планшетах необхідно вимкнути функцію «Автоматичне підключення до Wi-Fi».

Джерело: Interne