

Безпека мобільних пристроїв

Рекомендації для безпечного користування мобільними пристроями:

1. Встановіть PIN-код на SIM-картку для того, щоб у разі її втрати зломисники не змогли її використати з неправомірною метою.
2. Використовуйте двофакторну автентифікацію всюди, де можливо.
3. Активуйте у смартфоні функції «Знайти телефон». Якщо Ви втратите телефон, то надалі це може допомогти оперативно встановити місцезнаходження втраченого пристрою.
4. Не прикріплюйте всі банківські платіжні картки до єдиного телефонного пристрою. У разі втрати пристрою Вам не доведеться блокувати всі платіжні картки.
5. Встановіть складний пароль на доступ до пристрою та ввімкніть біометричну автентифікацію.
6. За можливості не вмикайте в телефоні функцію Smart Lock (розблокування за допомогою сторонніх пристроїв, як-от смарт- годинника). Зломисники можуть скористатися цією функцією для злому Вашого пристрою.
7. Слід вимкнути функцію виведення повідомлень на заблокований екран:
 - iOS: «Налаштування» → «Повідомлення» → «Показ мініатюр» → «Ніколи».
 - Android: «Налаштування» → «Повідомлення» → «Повідомлення (Екран блокування)» → «Приховати вміст».

8. Не створюйте та не пересилайте за допомогою месенджерів і повідомлень телефону скан-копії важливих документів, інтимні фотографії.
9. Якщо Вам хтось надсилає повідомлення або телефонує з проханням термінового переказу коштів, візьміть паузу, все добре обдумайте. За можливості передзвоніть іншим особам, пов'язаним із запитувачем, а також йому самому, та переконайтеся, що це саме та особа, про яку Ви думаєте. У подібних ситуаціях намагайтеся не пересилати кошти на карти чи електронні гаманці — краще передати їх особисто.
10. Якщо змінюється номер мобільного телефону, потрібно не забути перереєструвати всі наявні облікові записи на новий номер.
11. Якщо телефон було втрачено, потрібно терміново звернутися до оператора телекомунікацій та заблокувати SIM-картку й банківські платіжні картки. Надішліть повідомлення на сайти мікрофінансових установ про те, що Ваш телефонний номер було втрачено. У разі потреби зверніться до поліції. Повідомте про інцидент безпосереднього керівника та особу, яка відповідає за безпеку у Вашому підрозділі. Поділіться з колегами досвідом розв'язання інциденту, пов'язаного з порушенням інформаційної безпеки.

Передавання вживаних мобільних пристроїв іншим особам

Якщо Ви хочете комусь продати старий мобільний телефон, то майте на увазі: навіть видалені персональні дані з такого пристрою можна відновити.

Існує реальний приклад, як за допомогою спеціалізованого програмного забезпечення для криміналістичного дослідження мобільних пристроїв було знято образ даних вживаного смартфона. За

результатами пошуку інформації, в образі вдалося виявити:

- Паролі до точки доступу Wi-Fi та електронної пошти.
- Частина листування в соціальних мережах.
- Окремі фотографії, які зберігалися у смартфоні.

Також вдалося повністю відновити телефонну книгу до її видалення.

Для власної безпеки потрібно або взагалі не передавати іншим особам свої старі мобільні пристрої, або використовувати спеціалізоване програмне забезпечення для видалення персональних даних.

Передавання контактної інформації іншим особам

Взагалі слід якомога менше ділитися своїми персональними даними з іншими особами. Оскільки зазвичай телефонний номер прив'язаний і до електронної пошти, і до різних соцмереж, то за допомогою спеціалізованих сервісів можна зібрати повне досьє на конкретну людину.

З якою метою зловмисники можуть використати зібрану інформацію?

Шахрайство	Дискредитація	Шантаж
Створення умов для масштабної атаки на об'єкти, що пов'язані з жертвою		

Зібравши інформацію про Ваше коло спілкування, зловмисники можуть використати систему підміни параметра **Caller ID** (**Caller ID Spoofing**). Далі порушники можуть зателефонувати Вам із будь-якого знайомого номера, наприклад, близької особи або керівника. Якщо ж Ви не виявите підміну номера, це може призвести до незворотних наслідків.



Підміна CallerID