Безпека мобільних пристроїв

План лекції

Вступ
1. Блокування доступу до пристрою
2. Безпечна робота в мультимедійних засобах спілкування
3. Передавання вживаних мобільних пристроїв іншим особам
4. Передавання контактної інформації іншим особам
5. Захоплення номеру телефона
6. Шкідливе програмне забезпечення

Висновки

Рекомендована література

Основна

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: https://univd.edu.ua/science-issue/issue/4315.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 262 с.

Допоміжна

5. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
6. Про електронні комунікації: Закон України від 16.12.2020. *Офіційний вісник України.* 2021. № 6 (21.01.2021). ст. 306.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.

Текст лекції

Вступ

Сучасний комунікатор має не тільки функціонал телефону!
У ньому органічно поєднуються можливості:

- комп'ютера;
- кредитної картки;
- пристрою управління;
- мультимедіа;
- засобу зв'язку.

Така універсальність, з одного боку, робить зручнішим виконання повсякденних завдань, а з іншого – створює загрозу одномоментної втрати великої кількості персональних даних. В окремих випадках така втрата може стати критичною.

Кілька років тому бізнесмен ледь не втратив мережевий бізнес, який розбудовував кілька років. Спочатку зловмисники захопили управління його мобільним номером. У подальшому з використанням номеру телефону бізнесмена було одержано доступ до його електронної поштової скриньки, через яку було захоплено адміністративну панель домена, який було перереєстровано на інший обліковий запис. Для зміни паролю для доступу у даному випадку було встановлено двофакторну автентифікацію. А оскільки зловмисники захопили номер телефону бізнесмена, то, відповідно, стало можливим управління доменом. У нашому випадку бізнесмен вчасно звернувся до поліції, відповідних провайдерів та реєстраторів, завдяки чому через деякий час йому повернули облікові записи. Але такий результат буває далеко не завжди.

Під час користування смартфоном ви повинні постійно враховувати загрози, які особливо часто реалізуються за недбалого ставлення до вимог безпеки. Наслідки реалізації таких загроз можуть не тільки вплинути на вашу персональну безпеку, а й скомпрометувати підрозділ, в якому ви працюєте, а інколи й державу в цілому.

Давайте розглянемо кілька типових ситуацій, які можуть призвести до небажаних наслідків.

1. Блокування доступу до пристрою

Якщо ви залишаєте телефон без особистого нагляду, не забудьте його заблокувати надійним паролем або біометричним замком. В останньому випадку йдеться про використання як засобу автентифікації відбитку пальця або обличчя. У разі недотримання цих простих вимог зловмисники можуть не тільки захопити управління вашим телефоном, а й швидко авторизуватися у месенджерах з вашими обліковими даними, поштових сервісах, системі онлайн-банкінгу тощо. В останньому випадку ви можете не тільки втратити персональні дані, а й постраждати фінансово.

В одній з областей України зловмисник заволодів телефоном працівниці державної установи. У подальшому за допомогою системи онлайн-банкінгу він привласнив з її банківського рахунку 40 тис. грн. Поліція встановила особу зловмисника, яким виявився неодноразово засуджений за майнові злочини молодик. Йому повідомили про підозру одразу за двома статтями Кримінального кодексу України: ч. 1 ст. 187 «Розбій» та ч. 2 ст. 185 «Крадіжка».

Може трапитися, що ви навіть не помітите, як стали жертвою зловмисника. А в цей час ваші облікові записи будуть успішно використовуватись з протиправною метою (рис. 1).

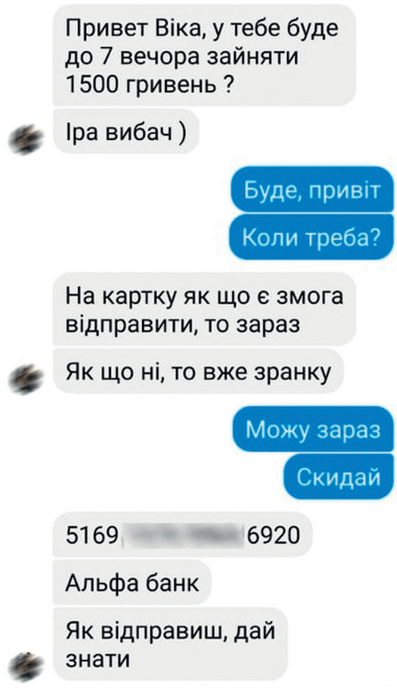


Рис. 1. Використання шахраями захоплених облікових записів

Здійснюючи атаку, шахраї можуть вивчати жертву для того, щоб бути більш переконливими. Найбільш простий приклад цього, коли зловмисник листується з потенційною жертвою тією самою мовою, якою жертва вела листування із захопленим обліковим записом (рис. 2).

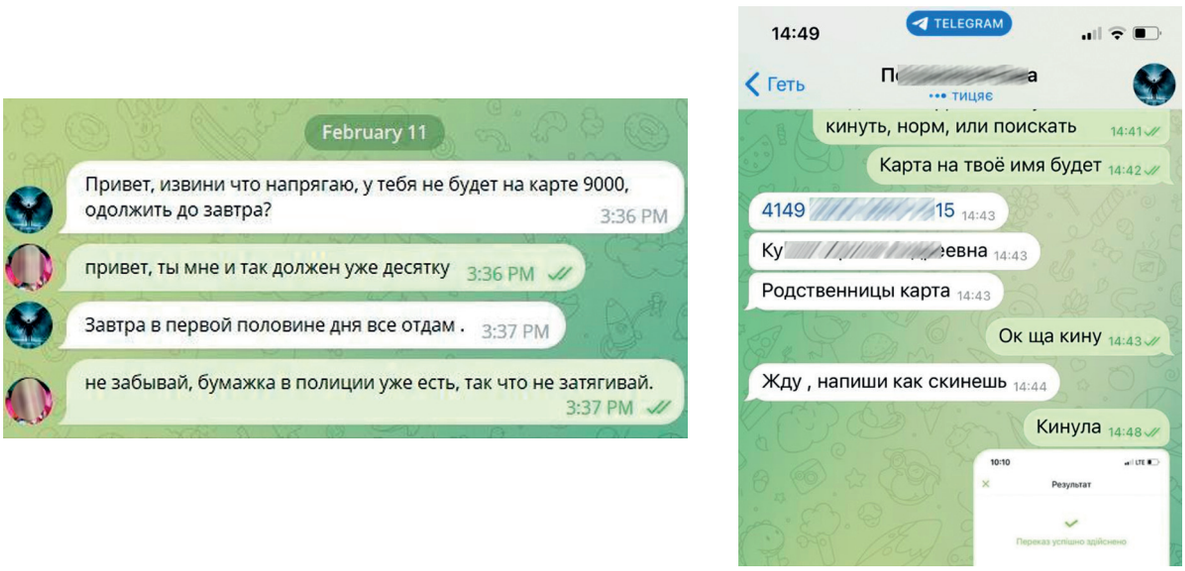


Рис. 2. Приклад спілкування зловмисника від імені захопленого облікового запису в Telegram

Для того, щоб частково зменшити ризики потрапляння в подібні ситуації, намагайтеся використовувати там, де це можливо, двофакторну автентифікацію, тобто коли для входу до якогось мережевого ресурсу потрібно ввести кілька паролів. Це може бути, наприклад, особистий пароль та додаткове підтвердження через СМС.

У будь-якому випадку, не ігноруйте повідомлення системи підтримки сервісів, у яких ви зареєстровані, оскільки в таких повідомленнях може міститися інформація про сторонній вхід до вашого облікового запису або про спроби такого входу.

Ранком на мобільний номер Сергія В. – одного з працівників обласної державної адміністрації – почали телефонувати його колеги і друзі та цікавитися, що у нього трапилося й для чого йому потрібні кошти. Не розуміючи, що відбувається, Сергій почав розпитувати колег про причину таких дивних дзвінків. Виявилося, що з його облікових записів у Skype, Viber та Telegram вночі почали надходити повідомлення про те, що йому терміново потрібні гроші, а також вказано номер банківської платіжної картки, куди слід їх переказати.
Як потім виявилося, попереднього дня Сергій забув телефон на роботі, й хтось, скориставшись його незапароленим пристроєм, спробував вчинити неправомірні дії.

У випадку потрапляння у згадані ситуації терміново:

- заблокуйте найбільш чутливі облікові записи (банківські, службові електронні кабінети);
- зверніться до особи, яка відповідає за безпеку у вашій установі (підприємстві, організації), та повідомте її про компрометацію облікових записів;
- якщо дозволяють налаштування, завершіть усі активні сеанси у ваших облікових записах та змініть паролі.

Для того, щоб пересвідчитись, що ваші облікові дані не скомпрометовано, скористайтеся одним або кількома з наведених сервісів:
https://breachalarm.com/
https://ghostproject.fr/
https://haveibeenpwned.com/
https://leakcheck.appspot.com/
https://monitor.firefox.com/
https://sitecheck.sucuri.net/
https://www.dehashed.com/

Крім наведеного, зловмисники здатні, скориставшись вашим незаблокованим пристроєм, одержати доступ до його історії, а також до історії вже існуючих облікових записів. Це може дозволити порушникам встановити місця вашого частого перебування, ваші коло інтересів, фінансовий стан тощо.

Спробуйте скористатися ресурсом takeout.google.com, який призначений для завантаження історії облікового запису Google. Як запитуваний обліковий запис використайте активний запис для телефону під управлінням операційної системи Android.

2. Безпечна робота в мультимедійних засобах спілкування

Залишення незаблокованим телефонного пристрою не є єдиною загрозою. Сьогодні телефон часто використовується не тільки для класичного мобільного зв'язку, а й також як комп'ютер, на якому встановлено різні мультимедійні засоби спілкування. Найбільш поширеними месенджерами, як правило, є Telegram, Viber, WhatsApp.

Деякі з наведених засобів дозволяють паралельне підключення з кількох пристроїв: комп'ютера, телефона, планшета. З одного боку, це досить зручно для користувача, а з іншого – створює додаткові ризики з точки зору безпеки. Якщо, наприклад, ви авторизуєтесь зі стороннього пристрою у своєму

обліковому записі та випадково забудете вийти з нього при завершенні роботи, то існує ризик подальшого використання зловмисниками облікового запису з неправомірною метою.

Найбільш часто не виходять із своїх облікових записів вдома, на робочому місці, у місцях проведення інструктивних занять, у комп'ютерних класах навчальних закладів, у комп'ютерах колег або знайомих, які використовувалися з метою вирішення якихось короткострокових завдань. Ще однією, вельми поширеною помилкою є перехід за неперевіреними посиланнями, які вам надсилають у засобах спілкування. Крім вірусів, такі посилання можуть містити перехід на фішингові сервіси, призначені для введення в оману користувачів. На сьогодні існують дуже велика кількість подібних рішень не тільки для веб-сайтів, а й для заволодіння управлінням месенджерами, що є вкрай небезпечним.

Наприклад, якщо у месенджері Telegram вам надійде повідомлення такого вигляду:

https://drive.google.com@fdsgdxsfdfdgvcg.tw,

то з першого погляду воно може здатися безпечним, адже є посилання на захищене з'єднання https зі справжнім сайтом Google. Однак, насправді, при натисканні на таке посилання у браузері відбудеться переадресація на сайт зловмисника fdsgdxsfdfdgvcg.tw.

Фішингове посилання може виглядати і не так незрозуміло, як уже наведене (рис. 3).

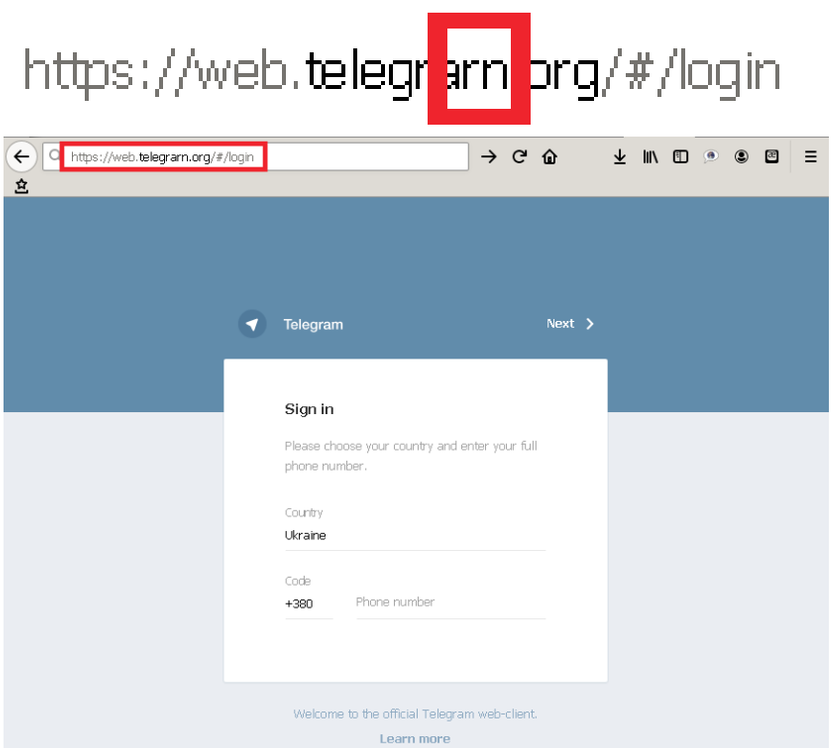


Рис. 3. Приклад фішингового сервісу Telegram

Враховуючи викладене, при переході за посиланнями, де вас просять ввести якісь дані, уважно передивіться текст посилання на предмет його справжності.

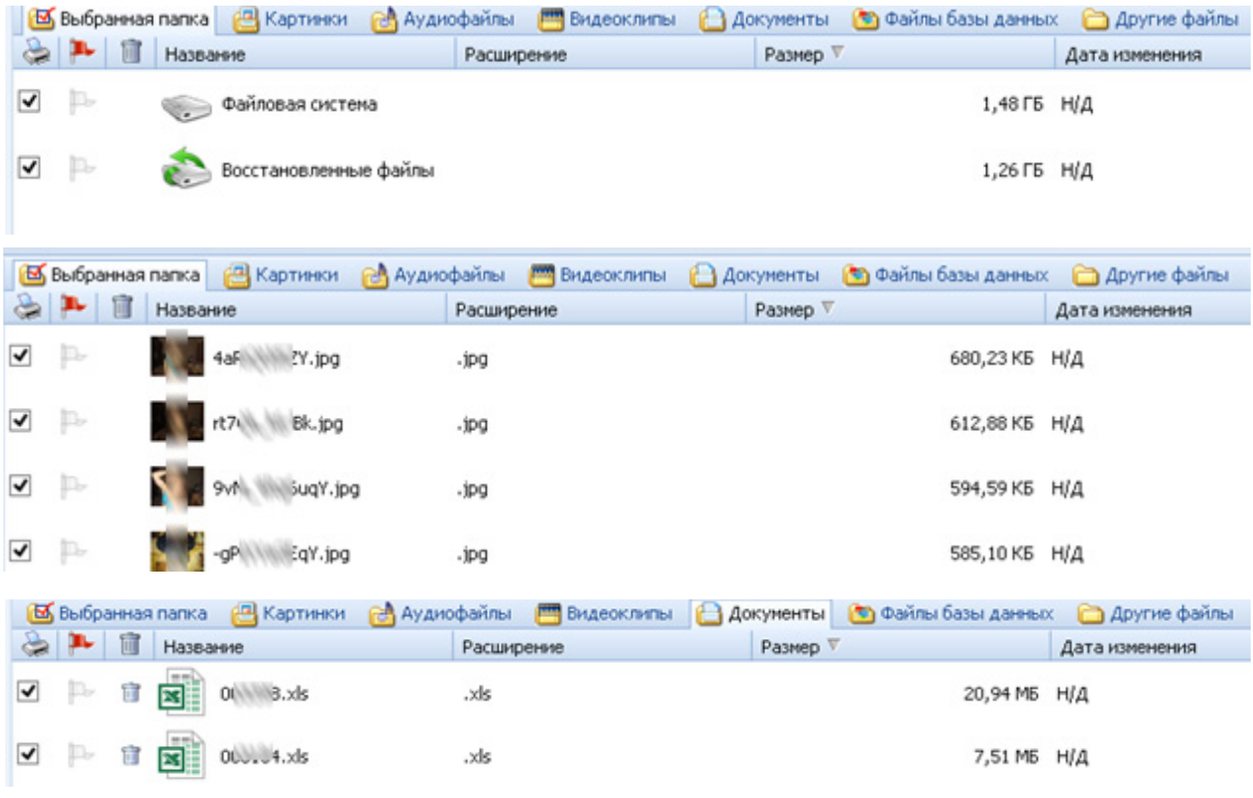
3. Передавання вживаних мобільних пристроїв іншим особам

Досить необачно вважати, що описані загрози є вичерпними. Уявіть ситуацію: ви хочете придбати новий телефон, при цьому вважаєте за доцільне одержати якісь кошти від продажу старого. Тому ви виставляєте його на продаж через систему OLX або просто продаєте на ринку.

Така ситуація трапляється досить часто, проте мало хто замислюється про те, що разом зі старим телефоном новий покупець може одержати доступ до ваших персональних даних.

Продемонструємо це на практиці.

Через систему OLX придбано вживаний смартфон марки LG, у якому попереднім власником було видалено усі персональні дані. За допомогою спеціалізованого програмного забезпечення для криміналістичного дослідження мобільних пристроїв було знято образ даних смартфону. За результатами пошуку інформації в образі вдалося виявити паролі доступу до точки доступу Wi-Fi та електронної пошти, частину листування в соціальних мережах, окремі фотографії, які зберігалися у смартфоні, повністю відновлено телефонну книгу до її видалення тощо (рис. 4).



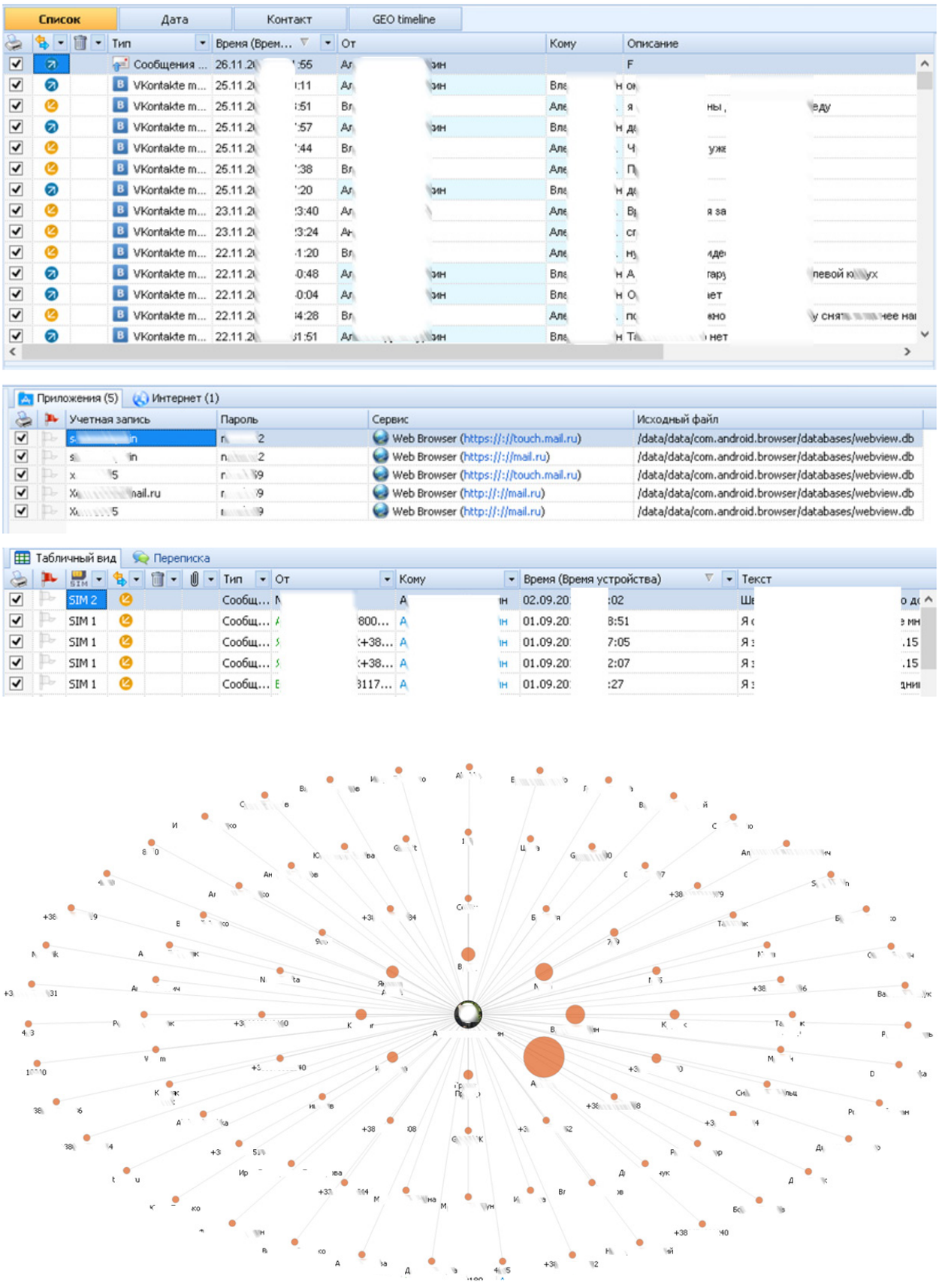


Рис. 4. Результати відновлення даних з мобільного пристрою

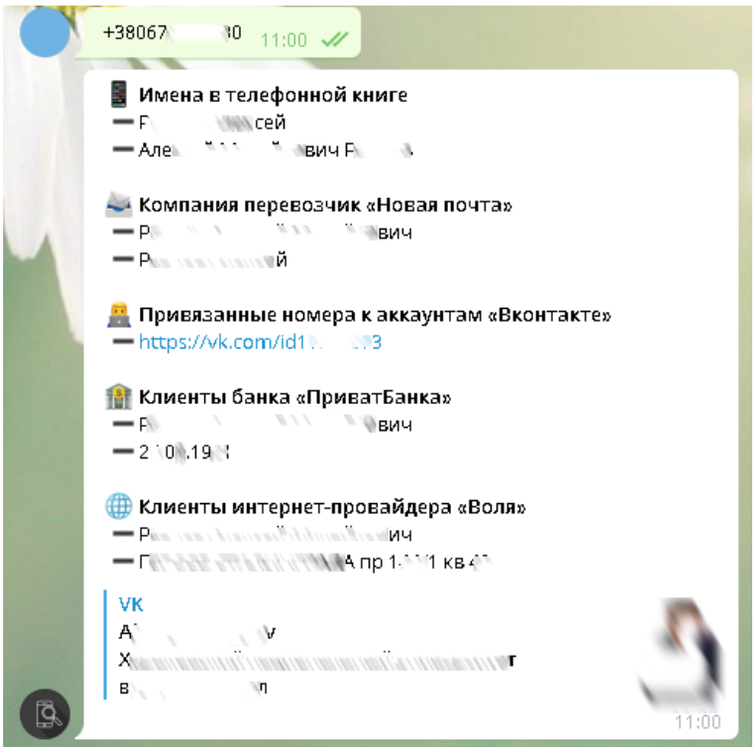
Для того, щоб унеможливити подібні ситуації, потрібно або взагалі не передавати іншим особам свої старі мобільні пристрої, або використовувати спеціалізоване програмне забезпечення для видалення персональних даних. Крім наведеного, під час продажу власне мобільного пристрою ви можете стикнутися з іншими загрозами, які реалізуються знов таки через мобільні пристрої.

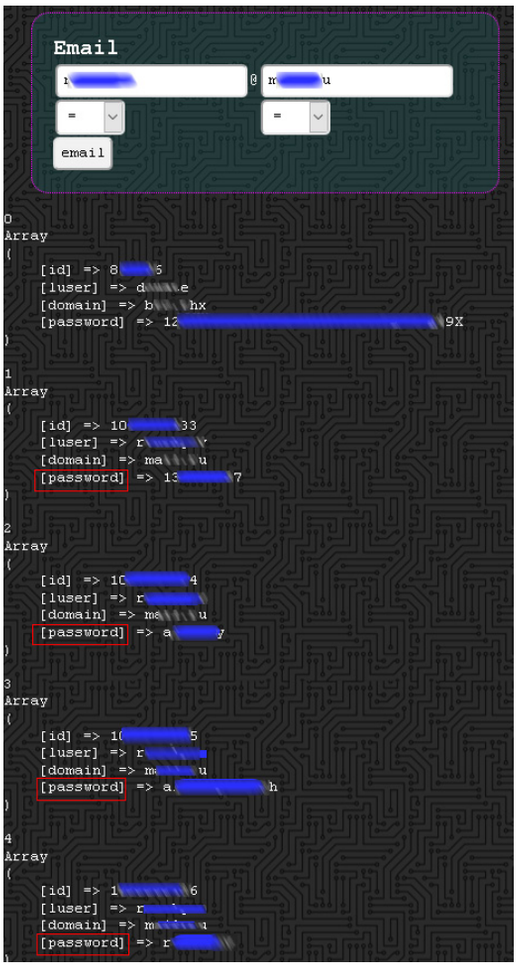
Мешканка Львова Тетяна Л. вирішила продати свій мобільний телефон Samsung S8 через систему OLX за 5000 грн. За деякий час до неї надійшла пропозиція придбати телефон від дівчини Аліни за 4800 грн. Телефон домовилися відправити поштою післяплатою до м. Одеса. Наступного дня до Тетяни зателефонував чоловік, який представився працівником служби технічної підтримки поштової компанії, та повідомив про помилку у введенні даних отримувача і про те, що зараз вони їх виправлять, а Тетяні потрібно продиктувати СМС із підтвердженням цієї операції.
За допомогою цього коду шахраї увійшли в особистий кабінет Тетяни на сайті поштової компанії та скасували післяплату. Таким чином, ними було одержано телефон без оплати, а Тетяна втратила і телефон, і гроші.
Після подання скарги до поштової компанії її представник повідомив, що така ситуація трапилася в їх компанії вперше.

4. Передавання контактної інформації іншим особам

Взагалі слід якомога менше ділитися своїми персональними даними з іншими особами. Адже це теж підвищує ризик встановлення зловмисниками ваших повних персональних даних, які потім можуть бути використані з неправомірною метою.

На рис. 5 наведено приклад (особисті дані приховано), як, маючи суто телефонний номер особи, за допомогою спеціалізованих сервісів можна зібрати на неї повне досьє.





Report for phone: +38067******0

Facebook checker
  email_part:
    - r******v@m***.ru
    - r******v@u**.net
  phone_part:
    - +3806*******0
  exists: true
Instagram exists: true
Skype possible accounts
  skype_profile_uid: r**********
  skype_profile_deep_link:
  skype://r********?chat
  skype_contact_type:
  Skype4Consumer

Telegram
  firstname: O****i
  lastname: R*****
  telegram_profile_uid: 9*******8
  lastseen: 202*-1*-1*T14:05:45

Caller ID
  fullname:
  ****
  carrier: **********
  country_code: **

Рис. 5. Результати збирання даних про особу за номером телефону з використанням загальнодоступних мережевих сервісів

Одержана інформація може бути використана з різними цілями. Це – і шахрайство, і дискредитація, і шантаж, і створення умов для масштабної атаки на об'єкти, пов'язані з жертвою, тощо.

Зібравши інформацію про ваше коло спілкування, зловмисники можуть використати систему підміни параметру CallerID (Caller ID Spoofing). Відомими сервісами, які надають послуги із заміни CallerID, є spoofcard.com, spooftel.com. Далі порушники можуть зателефонувати вам з будь-якого знайомого номеру, наприклад, близької особи (рис. 6) або керівника. У випадку, якщо ви не виявите підміну номеру, це може призвести до незворотних наслідків.

Рис. 6. Підміна CallerID

5. Захоплення номеру телефона

При роботі з мобільними пристроями слід пам'ятати й про іншу небезпеку, яка виходить з недосконалості системи ідентифікації власника мобільного номеру. Йдеться про перереєстрацію зловмисником вашого номеру на своє ім'я через перевипуск SIM-картки. Очевидно, що заволодівши вашим мобільним номером, зловмисник здатен реалізувати наведені вище загрози, а також використовувати цей номер з неправомірною метою для вирішення поточних завдань.

Увечері державний службовець Галина П. одержала SMS від свого оператора про те, що відбувається заміна її SIM-картки. Вранці зв'язок припинився. Галина звернулася до сервісного центру мобільного оператора, де їй відновили телефонний номер протягом двох годин. Проте за цей час відбулося списання грошей з її банківського рахунку через систему онлайн-банкінгу.

У цьому прикладі зловмисник скористався системою відновлення мобільного номеру, алгоритм роботи якої базується на тому, що оператору потрібно вказати:

- номери, з яких найчастіше телефонували на відновлюваний номер;
- коли було здійснено останнє поповнення балансу;
- з якими номерами відбувалися останні з'єднання.

На теперішній час відповідно до ч. 2 ст. 107 Закону від 16.12.2020 «Про електронні комунікації» відновлення послуг у разі втрати електронних ідентифікаційних засобів знеособленим (анонімним) абонентом (у тому числі SIM-карти, e-SIM, налаштування інтернет-роутера тощо) здійснюється за умови ідентифікації цього абонента у постачальника електронних комунікаційних послуг та надання персональних даних. Разом з тим ніхто не заважає зловмисникам залучити для процедури відновлення особу-посередника з паспортом, яка за певну винагороду погодиться відновити SIM-карту на своє ім'я.

Якщо вам часто телефонують з невідомих номерів, раптово поповнюють баланс, це може свідчити про підготовку до зміни номеру.

Для того, щоб убезпечитись від вказаної ситуації, потрібно прив'язати свій телефонний номер до паспортних даних. Крім того, бажано для чутливих операцій використовувати телефонний номер, невідомий нікому, крім його володільця та оператора зв'язку, або про який обізнані тільки близькі особи. Якщо все ж таки ваш телефонний номер захопили, вам слід терміново спробувати заблокувати діючі банківські платіжні картки, а якщо це не виходить, спробувати зняти з них кошти у найближчому відділенні банку чи банкоматі.

Інколи користувачі мають упевненість, що вжили усіх заходів реагування. Проте, як показує практика, жодні додаткові заходи безпеки зайвими не будуть.

Зловмисники реалізували схему заволодіння коштами особи, які зберігалися в банку, який здійснює обслуговування без відділень. У власниці мобільного пристрою iPhone спочатку було вкрадено телефон. Власниця оперативно заблокувала його через Інтернет на сайті Apple та вирішила, що блокувати банківську платіжну картку не має сенсу, оскільки доступ до рахунку в банку можливий тільки зі знанням PIN-коду. Проте зловмисники перевели вкрадений пристрій в режим польоту, а згодом підключили його до мережі Інтернет через свій маршрутизатор, на якому було обмежено доступ до сервісів Apple. У той же час банківські застосунки продовжували працювати. Відтак, викрадачам вдалося вивести більше 70 тис. грн з рахунків жертви.

6. Шкідливе програмне забезпечення

Украй небезпечним, з погляду безпеки, є потрапляння на мобільний комунікатор шкідливого програмного забезпечення. Такі програми можуть виконувати різні функції. У будь-якому разі вони здатні скомпрометувати не тільки власне систему, в якій вони запущені, а й її власника.

Нерідко шкідливе програмне забезпечення здатне спричинити неприємні наслідки у вигляді зашифровки даних телефону, перехоплення автентифікаційних даних, надсилання повідомлень на платні номери, оформлення платних підписок на різні сумнівні сервіси, використання пристрою для скоординованої атаки на різні об'єкти тощо (рис. 7).

Рис. 7. Приклад роботи вірусу

Кілька років тому було зламано телефон одного з найбагатших людей світу за допомогою спеціального відеофайлу в месенджері WhatsApp. За кілька годин після злому зі скомпрометованого телефону було викрадено кілька особистих файлів, а фотографії бізнесмена було передано одному з таблоїдів.

Враховуючи викладене, намагайтеся ніколи не встановлювати програмні рішення з неперевірених джерел. Інсталюйте антивірусне програмне забезпечення на свій пристрій. Не намагайтеся без крайньої необхідності отримати права суперкористувача root на своїх мобільних пристроях. З одного боку, рутінг дає можливість користувачеві зняти обмеження виробника чи оператора комунікацій, проте з іншого – полегшує зловмисникам доступ до вашого пристрою.

Додаткові функції мобільного пристрою

Крім наведеного, візьміть за звичку вимикати в телефоні функції, які ви не використовуєте.

Так, якщо у вас налаштовано автопідключення до відомих точок доступу Wi-Fi, ви так само автоматично можете бути під'єднаним до підробленої точки доступу. У подальшому весь трафік Інтернет може бути пропущений через обладнання зловмисника. Це дозволяє порушнику примусово перенаправляти запити з вашого пристрою на свої ресурси (рис. 8). При цьому ви можете навіть нічого не помітити.

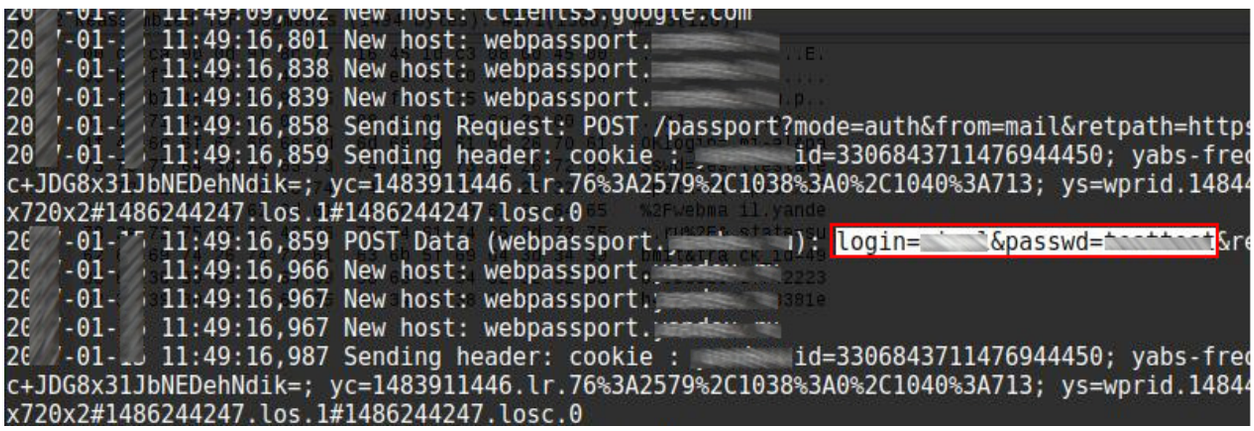


Рис. 8. Результат роботи програми mitmAP, призначеною для автоматизації створення безпровідної точки доступу та перехоплення трафіку

Необхідність вимикати невикористовувані функції стосується не тільки Wi-Fi, а й інших технологічних рішень. Увімкнений NFC-модуль, наприклад, може спричинити втрату грошових коштів або зараження вірусом.

> *У 2018 році працівники компанії Checkmarx продемонстрували, як зламати мобільний пристрій одним дотиком. Цей спосіб злому одержав назву NFCdrip і полягає в передачі зі спеціального пристрою або іншого смартфону через модуль NFC шкідливого програмного забезпечення на пристрій жертви.*

Варто відзначити, що від цілеспрямованих атак на мобільні пристрої не можуть бути застраховані навіть особи, обізнані з правилами інформаційної та кібербезпеки. Тому слід дуже прискіпливо ставитися до усіх незрозумілих подій з вашим пристроєм і ретельно обмірковувати свої дії в таких випадках.

Кілька років тому близько двадцяти керівників криптовалютних бірж Ізраїлю стали жертвами кіберзлочинців, які зламали їх облікові записи в Telegram. Попередньо зловмисники одержали доступ до стільникової мережі за кордоном та надіслали звідти оператору в Ізраїлі службове повідомлення про зміну місцезнаходження абонента-жертви. Після цього вони фактично змогли контролювати вхідні повідомлення жертви і таким чином зламати її облікові записи.
У даному випадку, очевидно, у жертв злочину не було встановлено двофакторної автентифікації, що дозволило зловмисникам захопити їх облікові записи.

Висновки

Усі наведені загрози не є вичерпними. Слід враховувати, що вони відображають тільки кілька ризиків. При цьому постійно з'являються нові вразливості та атаки, які можна відслідкувати тільки в процесі самоосвіти.

Тим не менш, для забезпечення прийнятного рівня безпеки слід дотримуватися базових правил:

1. Встановити PIN-код на SIM-картку для того, щоб у разі її втрати зловмисники не змогли її використати з неправомірною метою.
2. Де можливо, використовуйте двофакторну автентифікацію.
3. Активуйте у смартфоні функції «Знайти телефон». Якщо ви втратите телефон, то в подальшому це може допомогти оперативно встановити місцезнаходження втраченого пристрою.
4. Не прикріплюйте всі банківські платіжні картки до єдиного телефонного пристрою. У випадки втрати пристрою вам не доведеться блокувати всі платіжні картки.
5. Встановіть складний пароль на доступ до пристрою та увімкніть біометричну автентифікацію.
6. За можливості не вмикайте в телефоні функцію Smart Lock (розблокування за допомогою сторонніх пристроїв, наприклад, смарт-годинника). Зловмисники 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 усі наявні облікові записи на новий номер.
11. Якщо телефон було втрачено, потрібно терміново звернутися до оператора телекомунікацій та заблокувати SIM-картку, заблокувати банківські платіжні картки. Надішліть повідомлення на сайти мікрофінансових установ про те, що ваш телефонний номер було втрачено. У разі необхідності зверніться до поліції. Повідомте про інцидент безпосереднього керівника та особу, яка відповідає за безпеку у вашому підрозділі. Поділіться із колегами досвідом розв'язання інциденту, пов'язаного з порушенням безпеки.