ХІТ-ПАРАД
МОБІЛЬНОГО ШАХРАЙСТВА

Хіт-парад мобільного шахрайства

10 місце
ОТРИМАЙТЕ ВДВІЧІ БІЛЬШЕ!

- Один з найбільш примітивних, але, тим не менш, часто використовуваний спосіб обману. Вам приходить SMS такого змісту: «Сервер мобільного оператора Х. Перекажіть гроші на номер 8-ХХХ-ХХХ-ХХ-ХХ і одержите удвічі більше!». Знаючи, що любителів легкої наживи у нас в країні вистачає, обманщики тиснуть на психіку. Адже перевівши «на пробу» якихось 30 грн, ви можете отримати 60!. Відчувши можливість збагатитися, абонент переводить на вказаний номер всі кошти, що залишилися.

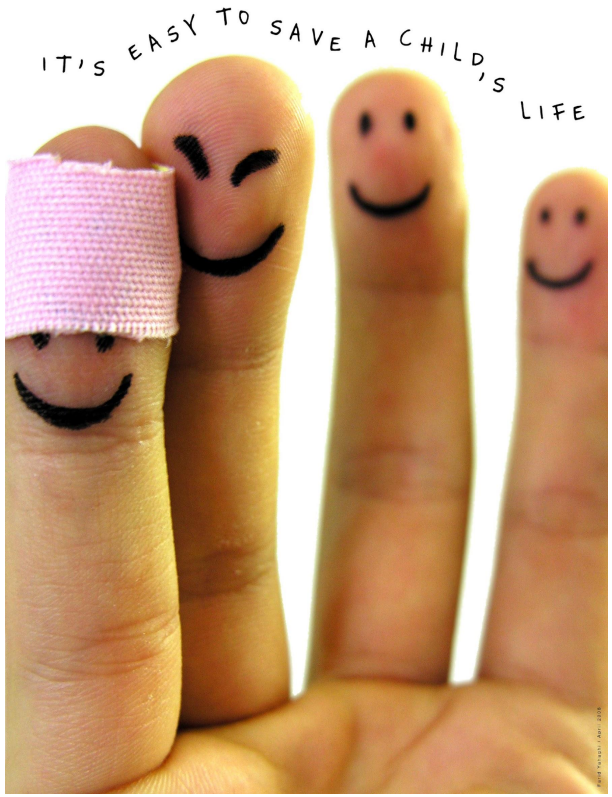
9 місце
ЖИТТЯ БЕЗ СПАМУ

- Абонентові приходить SMS з пропозицією відписатися від рекламної SMS-розсилки. Для того, щоб відписатися, пропонується відправити "безкоштовне" SMS певного змісту (найчастіше це набір цифр) на один з коротких номерів і перейти за отриманим у відповідь посиланням, для того щоб виключити номер із списку розсилки рекламних повідомлень.

- SMS на запропонований короткий номер виявляється платним і оцінюється в середньому $3-5

Хіт-парад мобільного шахрайства

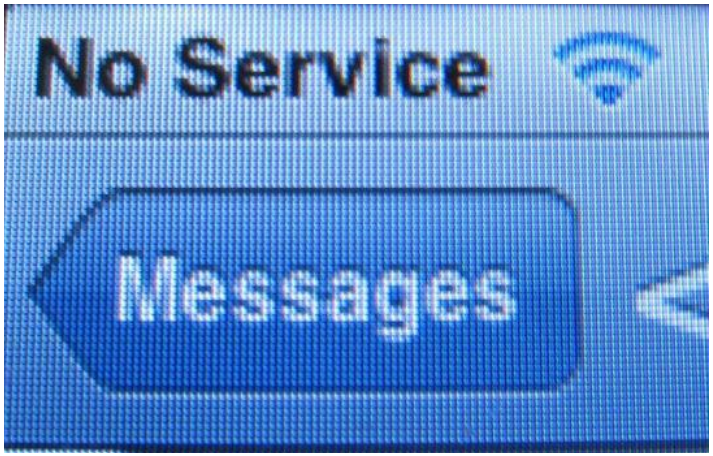
8 місце
ВРЯТУЙТЕ ДИТИНУ!



- Абонент отримує повідомлення з невідомого номера про необхідність знайти рідкісну групу крові для порятунку дитини. У повідомленні вказується номер телефону, дзвінки на який автоматично "полегшують" рахунок на 20-30 гривень

Хіт-парад мобільного шахрайства

7 місце
«ЗБІЙ» МЕРЕЖІ!



- У нас відбувся збій в системі. Ваш телефон через півгодини буде заблоковано на чотири дні.
- Як?! Що ж робити?!
- Ми зараз можемо швидко перереєструвати вашу SIM-карту в системі, наберіть на телефоні комбінацію * 150 * [050 ххх хх хх] * [200] # виклик.
- Тільки швидше, нам ще багато абонентів треба обдзвонити!
- Команда виявляється командою переказу грошей з одного рахунку на інший

Хіт-парад мобільного шахрайства

6 місце
ПОДЗВОНІТЬ БАТЬКАМ!

- На вулиці до вас підходять і просять дати подзвонити хворій мамі або дітям додому, посилаючись на акумулятор, що сів, і терміновість дзвінка. Через хвилину телефон повертається до Вас, а ось кількість готівки на рахунку сильно зменшується. Дзвінок здійснюється на платний номер.
- Зловмисники модернізували методи, й тепер можуть, начебто набираючи номер, встановити цифрову комбінацію, якою встановлюється програма, що без відома власника телефона спустошує рахунок (відправляє платні SMS, дзвінки на спеціальні номери)

Хіт-парад мобільного шахрайства

5 місце
ШУКАЮ РОБОТУ!

- Новий вид шахрайства: оголошення з пропозицією стабільної роботи з житлом і зарплатою 3000 дол на місяць.

- Для отримання інформації про роботу в них пропонується відправити SMS або зателефонувати на короткий номер (підвищена вартість SMS або платний автовідповідач). Абоненти, які відправили SMS, у відповідь на повідомлення отримували інформацію про те, що їх заявка прийнята в систему і чекає обробки. Однак, після відправки SMS на вказаний номер, з рахунку абонента знімалося 30 грн., Про які в оголошеннях не було ані слова.

Хіт-парад мобільного шахрайства

4 місце
ВИШЛІТЬ МЕНІ ГРОШЕЙ!

- Абонентові приходить SMS такого змісту: "Не можу тобі додзвонитися, немає грошей, перешли 5 гривень". Коли одержувач повідомлення намагається сам набрати вказаний номер, то чує, що абонент - поза зоною доступу. Деколи довірливі користувачі мобільних телефонів дійсно посилають суму незнайомцеві. Зайве говорити, що з цього номера їм ніхто більше не передзвонює

Хіт-парад мобільного шахрайства

3 місце
ПОВЕРНІТЬ МОЇ ГРОШІ!

- Користувач мобільного телефону одержує SMS-повідомлення про те, що хтось перевів на його рахунок певну суму грошей. Найчастіше вона невелика - 10-15 гривень. Через декілька хвилин приходить і інша SMS-ка, з повідомленням про помилку і проханням повернути гроші назад. Найчастіше такі повідомлення відправляються з Інтернету - в цьому випадку номер відправника не повідомляється, замість нього на дисплеї адресата з'являється короткий номер, максимально схожий на службове повідомлення. Природно, грошей на рахунку абонента не додалося, а жаліслива історія про фатальну помилку при передачі грошей другу - не більше ніж шахрайство. Втім, подібний виверт якраз і розрахований на порядність людей, які захочуть повернути гроші неуважному абонентові

Хіт-парад мобільного шахрайства

2 місце

ПОВЕРНІТЬ БОРГ!

- Абоненту приходить SMS: «Банк Х відмовив вам у видачі кредиту». Через декілька днів, коли абонент забуде про це повідомлення, йому дзвонять з незнайомого номера.
- Автовідповідач, представившись банком Х, говорить: «Нагадуємо Вам про необхідність погасити кредит. Хочете прослухати повідомлення ще раз, натисніть 1. Хочете зв'язатися з оператором, натисніть 2».
- Звичайно, абонент виходить на оператора, який правдоподібно описує ситуацію із заборгованістю за кредитом.
- Для детальнішого з'ясування обставин псевдооператор пропонує з'єднати абонента зі службою безпеки банку, завданням якої насправді є виманювання у переляканого абонента особистої інформації, номерів кредитних карток і ін. Не дивно, що після цього з карток починають зникати гроші. .

Хіт-парад мобільного шахрайства

1 місце
ВІТАЄМО! ВИ ВИГРАЛИ!

- Відбувається масова розсилка інформації абонентам (з використанням ПК) про нібито виграний приз, з пропозицією передзвонити за довідкою.
  Коли абонент дзвонить на рекомендований номер, начебто представники МТС йому повідомляють "радісну новину" про приз (домашній кінотеатр або навіть автомобіль). Щоби стати учасником акції, обов'язковою умовою є придбання ваучерів поповнення на суму 500 і більше грн, після чого треба повідомити секретні коди. Іноді можуть просити купити ваучери інших операторів. Після цього коди відразу використовуються зловмисниками для поповнення спеціально приготованих номерів, а далі перепродаються зі знижкою з використанням послуги переказу. Покупці коштів навіть не знають про їх шахрайське походження.

Бізнес-фрод - фрод в роумінгу

- Бувають випадки шахрайського заволодіння та подальшого використання номерів МТС для шахрайства в роумінгу. Інтернет рясніє подібними пропозиціями заробити: зареєструватися в інтернеті (договір з провайдером), далі "лити" дорогий трафік на певні контент-номери та отримувати за це відсоток.
- У 2009 р. в Україні з'явилася серйозна група, яка "присіла" на цю тему. Завдяки реагуванню МВС та ДБ МТС, 6 членів угруповання заарештовано в 2010 р.
- Зловмисники знаходили жадібних громадян, пропонували їм підключитися за винагороду і після підключення отримували стартові пакети. Хоча в контракті прописано, що абонент несе повну відповідальність за рахунками.
- Далі зловмисники вивозили сім-карти в роумінг та встановлювали через ПК цілодобові багатоканальні з'єднання з потрібними контент-номерами, наганяючи вигідну статистику по трафіку. Обмін файлами про події роумінг-абонентів відбувається між роумінг-партнерами не в режимі он-лайн - на те і розрахунок.

Шахрайства з мобільними платформами

- Останнім часом найбільш поширеними є дві нові схеми обману:
- Абонент завантажує додаток (наприклад, браузер Opera mini) на свій Android-телефон або iPhone, використовуючи неофіційний онлайн-ресурс. Встановлений додаток під виглядом поновлення щоразу самостійно відправляє SMS на різні короткі номери – вартість відправки становить від 9 до 50 грн. Складність полягає в тому, що абонент не може побачити відправлені SMS на смартфоні. Дізнатися про це він може, тільки проаналізувавши стан свого мобільного рахунку.
- При переході за посиланням у мобільному браузері смартфона відкривається сторінка з пропозицією оновити одну із встановлених програм. Виглядає сторінка цілком як справжня, однак, її адреса несуттєво відрізняється від адреси розробника програми. Якщо продовжити «оновлення», то в пам'ять смартфона буде встановлено зовсім іншу програму, метою якого може бути крадіжка конфіденційної інформації власника апарату, або відправка з його номера платних SMS.
- Якщо ви зіткнулися з одним з описаних випадків, необхідно негайно видалити із системи встановлений додаток, або звернутися в найближчий сервіс-центр виробника смартфона. МТС наполегливо рекомендує користувачам смартфонів на базі ОС Android та iOS встановлювати програми лише з офіційних джерел.

“Шахрайські” перспективи

- Згідно з пропонованими змінами до законодавства, в майбутньому будуть блокувати телефони, які внесені до “сірого/чорного списку IMEI-кодів”. Тобто, ті, які ввезені в Україну нелегально або ж украдені.
- Не виключено, що появиться окрема “сфера послуг”, в рамках якої шахраї пропонуватимуть “легалізувати” телефон. Цілком ймовірно, що окрім “виведення з чорного списку”, зловмисники вчинятимуть й інші незаконні дії, внаслідок яких довірливий клієнт розкриє приватні дані або ж позбудеться певної суми з рахунку. Це можуть бути нелегально завантажені програми, які без відома власника будуть використовувати трафік чи викрадати потрібні шахраям дані (паролі, номери банківських карток тощо).

МОБІЛЬНЕ ШАХРАЙСТВО І ЯК З НИМ БОРОТИСЯ

Види мобільного шахрайства

Дохід за рахунок оператора	Дохід за рахунок абонентів

Мобільне шахрайство

Щоденна робота **служби безпеки**: інформаційна й економічна безпека

Програмне забезпечення **Integrated Revenue Management**™, яке дає змогу мінімізувати фінансові ризики й попереджувати втрату прибутку

Програмне забезпечення **FraudView**®, яке дає змогу в режимі реального часу відстежувати й запобігати випадкам шахрайства через сервіси оператора

Уважність

Інформування: попереджувальні написи на ваучерах поповнення

Інформування: ЗМІ

Інформування: сайт компанії

Взаємодія з правоохоронними органами

Взаємодія з іншими операторами зв’язку

Проблеми в протидії шахраям

- Для використання правоохоронцями технічних засобів документування, необхідно заводити оперативно-розшукову справу (ОРС), в ході якої треба отримати судове рішення про відстеження місця знаходження зловмисника. Законність заходів та подальше ведення ОРС курується органами прокуратури. Заводити ОРС можна для розслідування тяжких і особливо тяжких злочинів, під ознаки яких такі дії шахраїв підпадають умовно. Кримінальну справу (КС) можна заводити якимось одним територіальним органом, за місцем вчинення злочину(там, де постраждав абонент). Абонентів обманюють по всій країні на невеликі суми (відповідно, формально для порушення КС потрібно близько десятка заяв щодо одного конкретного шахрая). До того ж, обдурені абоненти живуть у різних місцях, що становить додаткову проблему з їх опитуванням для протоколів.
- Друга проблема - українські правоохоронці поки що не мають високотехнологічного й дорогого устаткування для оперативної протидії мобільним шахраям.

Пам’ятка абонентам

Не розкривайте особистої інформації невідомим особам

Не спокушайтеся на легку наживу!

Будьте уважні щодо номерів, з яких Вам телефонують

Компанія МТС не проводить акцій, які вимагають розкриття кодів ваучера поповнення рахунку!

Дізнавайтеся більше інформації про акції та послуги!

При будь-яких підозрах на шахрайство, негайно повідомте оператора (111) або правоохоронні органи