Обережно – шахрайство

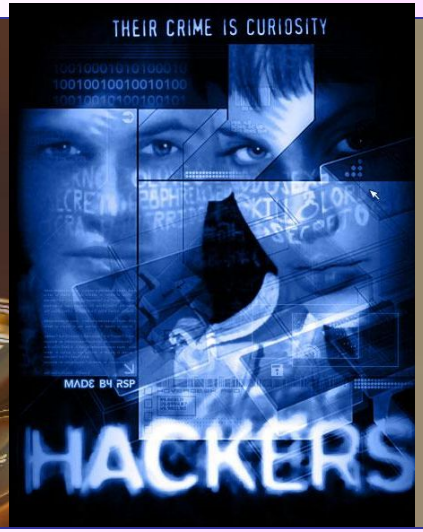
К.б.н. Полковенко О.В.

Шахрайство - злочин, що полягає в оволодінні державним, громадським, або особистим майном (або в придбанні прав на майно) шляхом обману або зловживання довірою. Очевидно, що людина, яка стала жертвою шахрайства зазнає сильний психофізіологічний струс.

Деякі найпоширеніші схеми шахрайства

Хто прагне проникнути до мого комп'ютера?

Кожен користувач Інтернету повинен мати чітке уявлення про основні джерела безпеки, що йому загрожують. Це насамперед діяльність *хакерів*, а також *віруси* та *спам*.



Хакер - тепер так називають людину, яка без дозволу проникає до чужої комп'ютерної системи з наміром викрасти або зруйнувати дані.

Комп’ютерне шахрайство

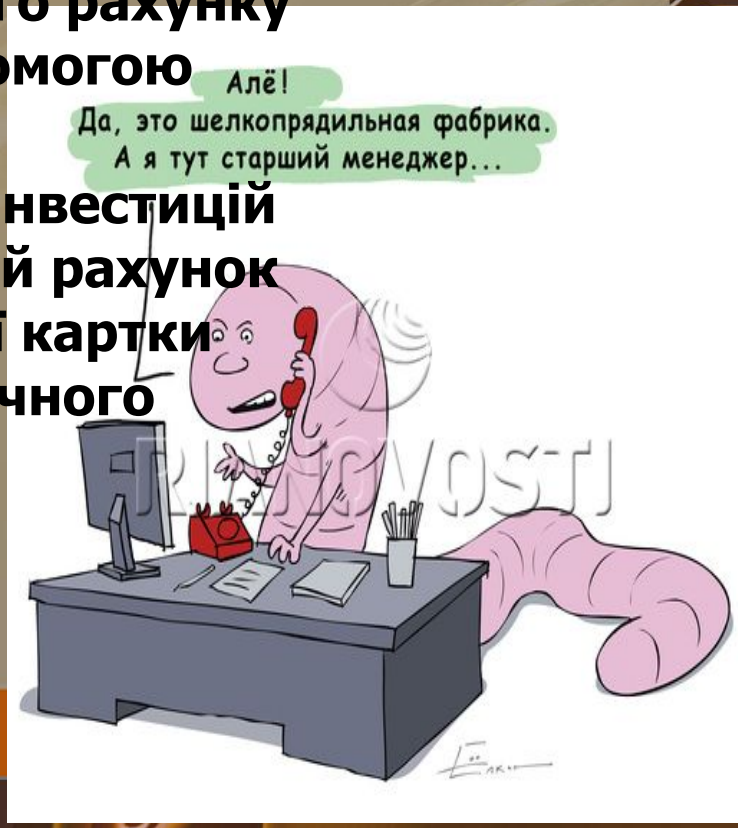
Фішинг — це технологія онлайнового шахрайства, яка використовується зловмисниками для отримання особистої інформації користувачів.

Ці дані використовуються в різний спосіб для отримання прибутку. Наприклад, розповсюдженою є крадіжка особистих даних, коли зловмисник викрадає особисту інформацію з метою виконання таких дій:

Отримання кредиту на ім'я іншої особи.

Отримання грошей із банківського рахунку та сплачування витрат за допомогою кредитної картки.

Переведення грошей із рахунку інвестицій або кредитної лінії на поточний рахунок і використання копії дебетової картки для отримання грошей із поточного рахунку в банкоматах світу.



Підроблені рахунки від служб доставки

Під час свят кіберзлочинці часто посилають підроблені рахунки і повідомлення про постачання товарів через відомі служби доставки, наприклад, від Federal Express, UPS або якісь повідомлення від Митної служби. Одержувач виявляє в електронній пошті лист з проханням вказати деталі кредитної карти для оплати рахунку за доставку, вимогу відкрити електронну версію рахунку онлайн або заповнити митну форму онлайн, щоб отримати пакет. Результатом може стати крадіжка особистих даних людини і, наприклад, установка шкідливого ПЗ на комп'ютері.

Електронні повідомлення, пов'язані з пропозиціями роботи

Лише у США рівень безробіття, що недавно піднявся до 10.2 відсотків, став найбільшим з 1983 року. У непростих економічних умовах шахраї полюють на тих, що зневірилися, шукають роботу, людей з обіцянками високооплачуваних робочих місць і можливостями роботи з будинку з хорошим прибутком. Після того, як зацікавлені люди надають свою інформацію і вносять «вступний внесок», хакери крадуть їх гроші замість того, щоб виконати обіцянки по працевлаштуванню.

Ви стали 1000-м відвідувачем

Вам приходить лист, наприклад, з Іспанії - або будь-якої іншої далекої країни, - але обов'язково англійською. У ньому вас вітають із тим, що одного разу, зайшовши на такий-то сайт, ви автоматично стали учасником розіграшу призів - і виграли! Приз - велика сума грошей або автомобіль. Щоб одержати його, вам треба всього лише переказати на певний рахунок якусь суму грошей, щоб оплатити доставку призу в Росію. Природно, зникають гроші безповоротно і безвісти. Відомі випадки, коли люди втрачали кілька тисяч доларів у надії на те, що от тепер їм нарешті вишлють їхній виграш.

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.

10

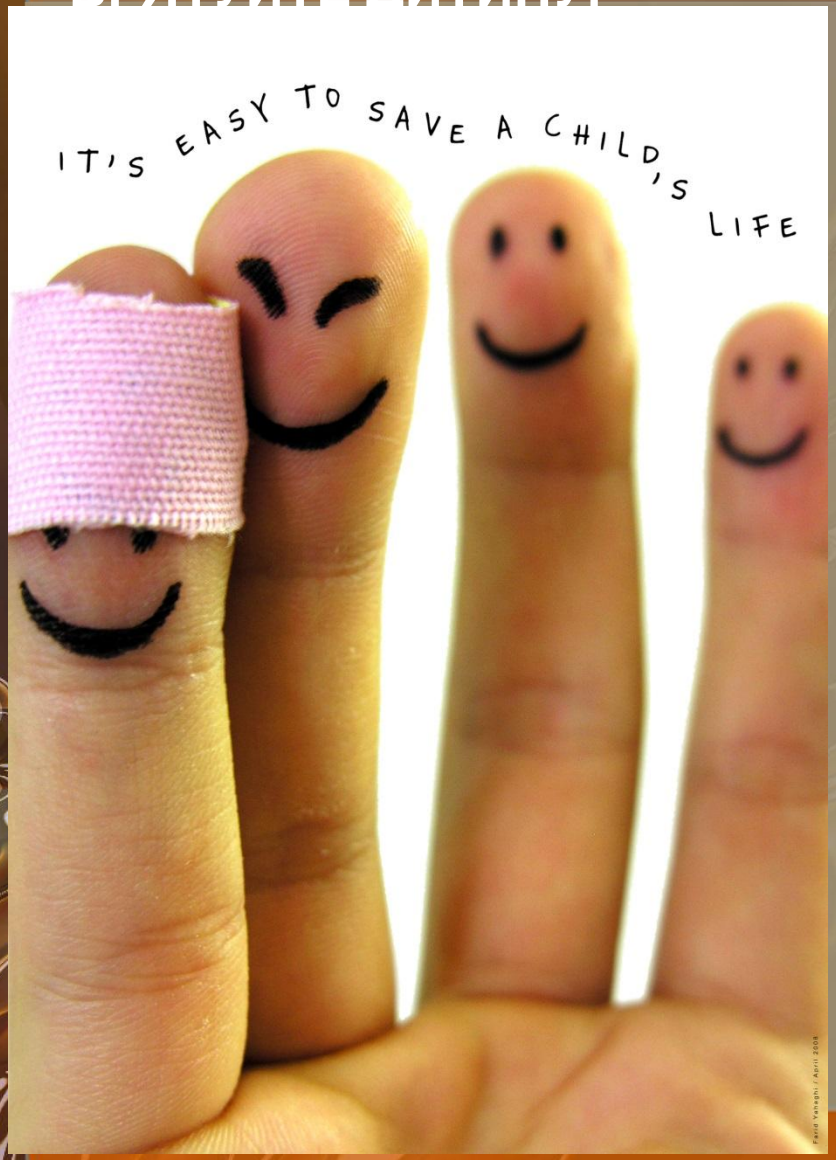
9 місце
ЖИТТЯ БЕЗ СПАМУ

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

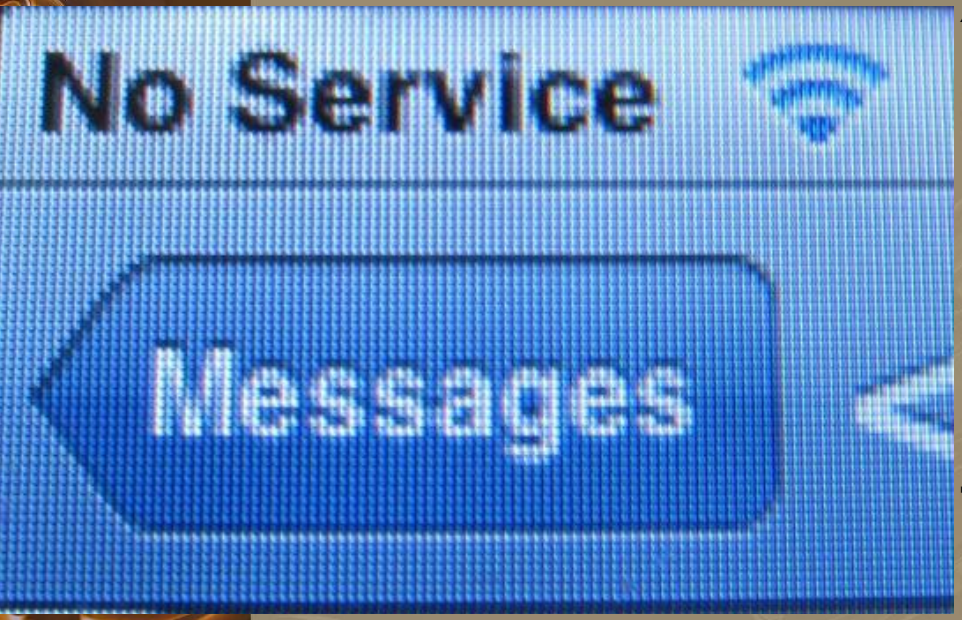
8 місце
ВРЯТУЙТЕ ДИТИНУ!



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 жалісліва 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

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!

ібувається 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.


Дякую за увагу!