АНТИКОР

Топ-теми:
- Арешт Єрмака
- Корупційна мафія Міндіча в Енергоатомі
- Напад Росії на Україну

Пошук...

НОВИНИ | КОМЕНТАРІ | ПОЗИЦІЯ | ДУМКА | ПОДІЇ | ВІЙНА | ВІДЕО | БЛОГИ

Як українців грабують в Інтернеті, банкоматах і кафе. Фахівці порадили, як врятувати свої гроші

Як українці грабують в Інтернеті, банкоматах і кафе. Фахівці порадили, як врятувати свої гроші

Читать на русском
Дизайн от Google дизайна в Google

Актуальність платіжних карток на часі важко переоцінити. Україні все частіше розраховуються ними за покупки не лише в інтернет-магазинах, але й у звичайних торгових мережах.

За даними Національного банку України кількість активних платіжних карток в Україні дещо зменшилася - на 3 тисячі за перший квартал 2015 року. Однак статистика за початок цього року показує, що кількість та сумми безготівкових операцій невпинно зростають - приблизно на 20% і 26% відповідно (у порівнянні з узгодженими даними за квартал 2014 року).

Та й готівку з карток українці почали знімати менше. Карткою дійсно легше розрахуватися у супермаркет, не треба кожного дня думати, скільки брати з собою грошей та перейматися, щоб у вас часом не витягли гаманець у метро чи іншому людному місці. Проте й у цей медаль є й інший бік - шахраї вже довели давно досяли того рівня, коли з легкістю можуть спустошити ваш банківський рахунок.

Для цього вам лише треба "засвітити" картку у будь-якому банкоматі, магазині або навіть кафе, же обнобуваши злодії. Читайте також: Міліція несподівано відпустила шахрайок, які "обнікали" пенсіонерці 50 тисяч гривень на літі папірці Шахрайства з платіжними картками є одним із видів кіберзлочинів та отримали назву кардінг. Через карткових злодіїв лише за другий півріччя 2014 року США втратили більше $ 36 млн.

В Україні цей вид шахрайства також набуває масового характеру. За даними київської міліції, у 2011 році було вкрито лише 9 кримінальних справ за фактами учинення кіберзлочинів, у 2012-му таких злочинів було вкрито вже 104, у 2013-му було вкрито 253, упродовж 2014 року працівниками управління боротьби з кіберзлочинністю було задокументовано 504 значних вказаної категорії, а станом на 1 квітня поточного року вже 49. І на перше місце серед різноманітних видів кіберзлочинів (наприклад, несправжні інтернет-аукціони, розсилка спам та створення вірусів) вийшло саме шахрайство з пластиковими платіжними картками.

Так про них не розповіли у першу чергу. Уралзиві банкомати Колишній судовий експерт, технічний експерт «Експерту Олександр Ураденко нарікає, що наразі просте приладдя, яке використовується для крадіжки грошей з карток, можуть виготовити навіть діти. А в інтернеті розповсюджується чимало відео з покроковими інструкціями на кшталт "зробіть сам". Скімінг (англ. skim - легко ковзати, знімати плівку) - крадіжка даних карти за допомогою спеціального пристрою - скімера. Зловмисники копіюють все інформацію з магнітної стрічки платіжної картки (ім'я власника, номер картки, термін закінчення її дії, CVV та CVC-коди), а дізнатися ПІН-код можна за допомогою мініі-камери або накладок на клавіатуру, встановлених на банкоматах. Такі пристрої можуть бути різним розмірів та мати будь-який вигляд. Скімери, які встановлюються на банкоматах, інтегують його деталі так, що клієнт бачу навряд чи зможе відрізнити в від справжніх.

Сам скімер - це накладка на картоприймачі. Під пластиковим корпусом ховається магнітна головка, що, як магнітофон касету, зчитує інформацію з картки, яка, своєю чергою, зберігається на невеличкому чипі. Такі скімери встановлюються у дуеті разом із відеокамерою, яка має записати процес введення і клавіатури ПІН-коду. Камеру разом із чипом для зберігання відео кожаать за окремою накладкою і можуть встановити як зверху над монітором банкомату, так і десь збоку - тут уже залежить від розташування клавіатури. На основі даних, зібраних скімером та відеокамерою, шахраї створюють матрицю, яка інтуїтив пластикову картку і ку потім (в процесі шахрайства) банкомат розпізнає як легітимну.

Захистити свій ПІН-код можна, прикривши рукою клавіатуру під час його введення, радять правоохоронці. Однак такий спосіб, зазначає технічний експерт Олександр Ураденко, не можна бути ефективним на 100%, адже для того, щоб вирахувати пароль, шахраю треба розглядіти лише три цифри, а ту, що лишилася, можна дізнатися шляхом простого підбору з трьох різних комбінацій. Замість камери можуть використовуватися і спеціальні накладки на клавіатуру, що запам'ятовують, на які цифри натискав власник картки, вводячи ПІН -код. За даними правоохоронців, шахраї часто вдаються саме до такого способу крадіжки ПІН-коду, проте накладку легко помітити.

"Наявність підкладної клавіатури дуже просто помітити, оскільки справжня клавіатура зазвичай лиго та вона кіяхли не буде виступати або відходити у деяких місцях від корпуса банкомата. А ось підкладну клавіатуру, яка встановлюється зловмисниками, можна легко знати, лише підвівши її з боку", - зауважив начальник київського управління боротьби з кіберзлочинністю МВС Руслан Олінюк.

Перед установкою скімера шахраї проводять так званий ретрайлінгі підбір: оцінюють район, відвідуваність, підхід до самого банкомату. "Обов'язково є люди, так званіداللول, які спостерігають за тим, хто вводить пароль. Інші можуть спеціально спровокувати ситуацію, щоб подивитися, як люди будуть реагувати. У народі це називається стратегічна розвідка. Потім вони вже вирішують, не можна сюди ставити скімер", - розповів технічний експерт Олександр Ураденко. Він додав, що шахраї зазвичай обирають таке місце, щоб банкомат стояв окремо, тобто не залежав ні від відвідувачів, ні від людей. Тож, щоб зберегти свої гроші, краще обирати банкомати, які розташовані у добре освітлених місцях, біля або у самих відділеннях банків, а також поблизу постів охорони або міліції (наприклад, у метро).

Однак інші шахраї обирають місця, де їхні підозрілі дії, здаваося б, легко помітити. Так, Олександр Ураденко зазначив, що є випадки встановлення скімерів на банкоматах у супермаркетах. Наприклад, підійшли дві людини. Один працює, щось клеїть (накладку зі скімером), а другий повернувся і каже: "Не підходьте, проводиться технічний огляд", - розповів експерт і додав, що установка та зняття скімера - швидка справа, яка займає близько 10 секунд.

Скімер і відеокамера працюють на звичайних акумуляторах від телефону, роботи вихи вистачає приблизно на добу, після чого шахраї знімають свої приладдя. Тож якщо раптом звичний банкомат видається вам підозрілим, то інтуїтивні накладки можна виявити, якщо посмикати найбільш "небезпечні" місця, наприклад, картоприймач. "Якщо якісь деталі відходять - це скімер або накладка з камерою", - додав експерт Олександр Ураденко. Серед інших порад, як знемогти риски стати жертвою шахраїв, експерт зазначають таке: - не рекомендується зберігати всі гроші на платіжній картці; - встановити лімітні на щоденне або разове зняття грошових коштів з картового рахунку; - підписатись на SMS-інформування про проведені трансакції; - у разі виникнення сумнівів уже після вводу ПІН-коду необхідно знати максимально можливу суму для того, щоб зловмисники не заволоділи вашими коштами, та терміново повідомити банківську установу для перевірки.

Крім того, у банках розповіли ТСН.ua, що наразі цирюко використовуються так звані антискімінгові накладки, які унеможливлюють встановлення скімерів на банкоматах. Також банківські спеціалісти рекомендують заноміяти чиповку картку, яка має підвищений рівень захисту. "Захист від підробки, оскільки інформація, записана у чипу, має криптографічний захист, який неможливо скопіюватиміяти", - зауважив начальник управління ідентифікації шахрайства департаменту ризик-менеджменту АБ "Укргазбанк" Роман Степанець.

"Скопіювати дані з картки з чипом набагато складніше. Якісь методи є, але у нас не було таких випадків на практиці", - зазначив директор з інформаційних технологій "Приватбанку" Дмитро Дубілет. Водночас спеціаліст наголосив, що єдиним недоліком чипової картки є її вартість.

"Не всі банки перейшли на картки з чипом, бо вона набагато дорожча за картку з магнітною стрічкою. І якби всі картки були замінені з чипами, для українців це обернулося б більш високими комісіями", - додав Дмитро Дубілет. Сумнівні кафе і магазини ЗІ скімером можна зіткнутися не лише під час роботи з банкоматом, а й у зовсім неочікуваних місцях. Так, скімером може виявитися звичайний на перший погляд термінал, через який сплачується покупка у магазині чи заживлення у кафе.

Шахрайська схема виглядає так. Ви приходите у кафе, вас обслуговує дуже ввічливий офіціант, а коли вж вже збираєтесь сплачувати рахунок і, на жаль, готівки у вас виявляться недостатньо, вм пропонуєте картку. Офіціант приносить вам термінал, через який проводить картку. Але в терміналі несправжній, тож він видає помилку. Це не виклякає підозр, оскільки подібні ситуації зі справжніми Wi-Fi терміналами - не рідкісне явище. Відтак офіціант вибачається та йде до бару начебто за іншим терміналом, а дорогою ховає свій пристрій.

Ваш ПІН-код він може підглядіти вже під час розрахунку через справжній термінал. У такому разі офіціанти ризикує бути викритим, оскільки йому треба десь ховати свій "термінал". Тож шахраї можуть використовувати й іншу схему з непрямітним принципом. Офіціант забирає вашу картку разом зіз рахунком на бар й у влучний момент проводить по її магнітній стрічці мініатюрним скімером, яїбудованим, наприклад, у перстень. ПІН-код він може отримати так само, як і в першому випадку. Варто зазначити, що мініатюрним скімером можуть використовуватися не тільки у кафе, але і в магазинах та супермаркетах, де таким терміналом просто замінюють справжній. Відтак скімером можуть бути й такими, що проводять платіж продавцю, наче справжні, але при цьому крадуть дані з вашої картки.

Для обох способів шахраїв, як правило, обирають доволі сумнівні заклади, вказали вони, не дуже ретельно ставляться до підбору персоналу і під їхнім носом можна вкрадіти будь-що. Так для втілення своїх коштів варто оминати подібні місця, які виклякають підозру. Інтернет-магазини Зарз електронна комерція займає вагомі позиці в економіці країни, тож популярним видом шахрайства з платіжними картками є несанкціоноване використання їх під час купівлі товарів або послуг у мережі Інтернет. У більшості випадків шахраям не доводиться вдаватися до якихось надуманих технологій, зазначають правоохоронці. Найчастіше вони розміщують фейкове оголошення, у якому за товар або послугу "продавець" вимагає переказати передплату. Після отримання коштів зловмисник не надсилає товар або не надає відповідної послуги. І, с шахраїв і більш складна схема.

Клієнту пропонують переказувати гроші на карткові рахунок "продавця" та дізнаються номер рахунку, персональні дані та номер мобільного телефону власника, начебто для вирішення питань, які можуть виникнути при перерахуванні коштів. Читайте також: На Полтавщині аферисти ошукали 250 клієнтів інтернет-магазина "У подальшому на мобільний номер власника картового рахунку телефонує особа, яка представляється працівником банківської установи та ставлячи запитання щодо надходжень, які очікуються, зазначає, що кошти не можливо буде зарахувати від юридичної особи у зв'язку з неактивацією відповідною функцією, та пропонує, що шляхом здійснення ряду дій біля найближчого банкомату зазначене питання можливо вирішити. У результаті здійснення таких дій, громадянин, не розуміючи їхньої суті, самостійно переказують кошти на рахунки шахраїв або активують функції, які надають шахраям можливість заволодіти грошовими коштами, що знаходяться на картковых рахунках громадян", - повісив начальник київського управління боротьби з кіберзлочинністю МВС Руслан Олінюк.

Щоб не стати жертвою такого злочину, правоохоронці пропонують українцям дотримуватись таких рекомендацій: Перевіряйтесь у надійності магазину або продавця, для чого потрібно зі всіхтелі з представником магазина або безпосередньо з продавцем за реквізитами, вказаними на веб-ресурсі. Провести у Мережі перевірку за назвою інтернет-магазину або за номером телефону продавця, з метою виявлення відгуків про цей сайт/от постраждалими або про особу. Перевірити вартість товару. Вас має настрожити, якщо вона набагато нижча, ніж в інших інтернет-магазинах. Зчитувати термін доставки та спосіб оплати товару. Перевірити у Мережі місце знаходження інтернет-магазину або особи-продавця (адресу, вказану на сайті). Оплату проводити товар краще за всіх здійснювати кур'єру під час отримання та після перевірки покупки. У разі якщо вам на мобільний номер телефону особа, яка представляється працівником банківської установи і вимагає повідомити персональну інформацію та інформацію по платіжній картці, у жодному випадку не надавайте запитувану інформацію, а краще зверніться до найближчого відділення вашої банківської установи та проконсультуйтесь із працівниками банку. Фішинг (де одним вкадом інтернет-шахрайства є фішинг (англ. рибоголінг, метод якого отримання доступу до конфіденційних даних користувача, зокрема, до реквізитів платіжної картки. Шахраї виконують спеціальні дані, наскорчи фішингові сайти під інтернет-магазини. Посилання на свій ресурс зміді надсилають на електронну пошту у спамерами або у SMS. Зловмисні сайт-двійник має веб-адресу, яка дуже схожа на адресу справжнього сайту. Проте іноді вірус може повністю підмінити URL. Відтак, необхідний користувач може "подорожувати" шахраям даної системі карток, навіть не помітивши цього.

"Буваютъ такі випадки, коли сайт є повною копією. Веб-адреса або схожа, або взагалі така ж сама, яка вірус: якщо ж чинок підмінив. І і коли вкрадіть свої дані на цей сайт, то ці дані вже використовуються шахраями на справжньому сайті. Але з іншого боку, банки тж не стоять на місці і навіть коли користувач потрапляє в таку ситуацію, і дане високий ймовірність, банк до виявлає за допомогою нетчнологіях. У або інших сонах і блокує таку інформацію", - розповів директор з інформаційних технологій "Приватбанку" Дмитро Дубілет. Роман Степанець, начальник управління ідентифікації шахрайства департаменту ризик-менеджменту АБ "Укргазбанк", запропонував для прикладу порівняти справжній сайт платіжної системи Visa та створений шахраями цар у 2011 році клон, де ідентичними були навіть значення коштних каналів і графічних елементах і можливості проблем у вексті тексту.

Серед порад, як не стати жертвою фішингу, банківські спеціалісти вказують таке: - Не переходьте за посиланнями у листах або SMS, надіслано начебто від імені банку. А якщо вже клікнули, то не вносьте у запропоновані форми свої особисті дані. Банки ніколи не надсилають таких листів з подібним проханням. Під час розрахунків у мережі користуйтеся надійними та перевіреними Інтернет-магазинами, а оплату краще здійснювати зі свого персонального комп'ютера і не користуватися з таких вкладках комп'ютерами в інтернет-клубах. Під час оплати в Інтернеті не надавайте свої особисті дані. Для проведення трансакції вистачить номера картки, строку дії та CVV-коду (трьохзначний код. Якщо вас просять назвати дату та рік народження, дівоче прізвище матері та інші особисті дані або надати різні комбінації цифр на телефоні, то ви маєте справу з шахраєм. Якщо вам часто доводиться оплачувати послуги в Інтернеті, варто відкрити спеціальну Інтернет-картку, що дозволить уберегти реквізити ваших основної платіжної картки. Встановіть картковий ліміт на суму та кількість операцій на оплату товарів/послуг в Інтернеті. Його можна легко змінювати за необхідності. Так ви ви втратите кагту, або ваші персональні дані будуть вкрадені, зловмисники зможуть скористатись вашими коштами лише в межах встановленого ліміту.

Використовуйте антивірусне програмне забезпечення із регулярно оновлюваними антивірусними базами. Телефонні шахраї Напрямці варто зладити ще про один простий шахрайський спосіб заволодіти персональних даних - телефоном. У цьому випадку аферисти не обіймають собі шахрайства чайте дейлоиець то не надушить зі скімерами, вони просто шукають довірливого клієнта банку. Дали банк ніколи за своєю ініціативою не дзвонить клієнтам для того, щоб дізнатися персональні дані - номер банківської картки, строк її дії, ПІН-код, СУС-код або надати слово (наприклад, дівоче прізвище матері). "Шахраї дзвонять, представляються службою безпеки банку або ще кимось і кажуть: "Вертелько скажіть пароль з SMS," Вертелько скажіть ПІН-код". Якщо ваш ваш телефонн "банк" і просить це назвати, то це шахраїв", - зазначив директор з інформаційних технологій "Приватбанку" Дмитро Дубілет.

Банківські представники заявляють, що відшкодовують гроші своїм клієнтам, які стали жертвами кіберзлочинців. Але водночас зазначають, що це відбувається у разі відсутності провини з боку клієнта. Оскільки довести факт своєї непричетності може бути складно, то для збереження власних коштів варто вивчити превентивними заходів і дотримуватися правил безпеки під час використання платіжної картки та її реквізитів в Інтернеті.

Скачко Ольга

ТСН

Теги: Мошенники | Мошенничество

Юлія Більченко
ВИТОСКОВИЙ РЕДАКТОР

03 червня 2015 р., 14:24 | Переглядів: 4256 | Коментарі: 0

Роздрукувати | Надіслати товаришу

Коментарі:

comments powered by Disqus

Важливі новини

ЦЕНЗУРА
ЯК ОБІЙТИ БЛОКУВАННЯ І ЧИТАТИ НАШ САЙТ

Останні новини

Фільтр: Усі новини | Не прочитані | Не коментовані

11:02 РФ відкрила по розвідувальному центру «Аврора»
10:57 Нічний обстріл Одеси: в місті пролунали серія вибухів
10:50 Суд скасував понад 116 тисяч гривень податків і штрафів за доходи з OnlyFans
10:44 Зеленський закликав посилити ППО після масованих ударів РФ «Ще раз нагадаю, всіх моїхо б не було»
10:38 Глава МЗС Німеччини приїде до Києва в центрі міста обвінчать рух
Підписуйтесь на наш канал в Telegram. Оперативні про головне
10:32 В Одеській області пошкоджено енергооб'єкти ДТЕК: в Одесі є перебої зі світлом
10:26 США запровадили 50% мита на частину алюмінієвих товарів після провалу переговорів (1)
10:20 У Херсоні внаслідок атаки дронів знищено торговельний центр (1)
10:14 Росіяни вбили людину та поранили сімох на Донеччині за добу (1)
10:08 Шахраї наскочили під Кіровоградом та вимагають «штраф» у криптовалюті
10:01 Росіяни вдарили дронами по складах на Запоріжжі: виникла пожежа
09:58 РФ атакувала Україну балістикою та 217 безпілотниками
09:52 Після атаки РФ на Кривий Ріг у лікарнях залишається 61 людина: 21 — у важкому стані
09:46 Росіяни знову атакували Чернігів: горіли приватний будинок, пошкоджені магазини (1)
09:41 В Одесі після нічної атаки зафіксовано перебої із світлом
09:36 У Кривому Розі провів розбір завалів торговельного центру (1)
09:30 У Миколаєві безпілотники атакували будівельний супермаркет
09:24 Німецька промисловість втрачає конкурентоспроможність у Берліні звинувачують Китай (1)
09:18 У Полтаві пролунали вибухи
09:12 У Чорному морі дрон атакував контейнеровоз BMS TEAM: 11 моряків врятували, один зник безвісти (1)
09:06 Дрони атакували Самарську область: виникли пожежі на НПЗ та в логістичному комплексі Ozon
09:00 Росіяни атакували Харківську десятками дронів: постраждали троє людей (1)

Теги новин

COVID-19 агресори Росии Атаки Війна Война ВСУ Вторжение Донецьк Трамп Донбасс ДТП Зеленський ЗСУ Київ Київ корпоративну порушення Напад Росії на Україну Нападение Россия на Украину окупанти окупанти Порошенко Путин Росія Россия сбу США Украина Україна ЧП Знищене корпоративну

Наші опитування

Чи вірите ви, що Донбас Донецьк зможе зупинити війну між Росією та Україною?
- Так, повністю зможе
- Частково зможе, але не відразу
- Ні, не зможе
- Це залежить від дій лідерів сторін
- Важко відповісти

Голосувати

Показати результати опитування
Показати всі опитування на сайті

2015-2026 © АНТИКОР — національний антикорупційний портал
Реклама на сайті • Наші партнери
Політика конфіденційності
Використання матеріалів сайту дозволено лише за наявності активного гіперпосилання на джерело. Ті права на тексти, зображення, фотографії та відеоматеріали належать їх авторам.

6.0/0.152