ІНФОРМАЦІЙНІ МАТЕРІАЛИ ДО КРУГЛОГО СТОЛУ
«Кіберзлочинність:
українські банки на лінії удару»

Згідно з оцінками Комісії з внутрішніх справ Палати громад парламенту Великобританії, втрати світової економіки від злочинів, скоєних за допомогою Інтернету, досягли суми в 388 млрд доларів на рік. «Тим самим кіберпростір обійшов за своїм розмахом світовий злочинний наркоринок, річний оборот якого оцінюються в 288 млрд доларів», - підкреслювалося в її нещодавній доповіді. «Небезпека з боку інтернет-злочинності зараз більш серйозна, ніж з боку ядерної зброї», - заявляв голова Комісії, депутат Кіт Ваз.

Як повідомляла Symantec (американська компанія з виробництва програмного забезпечення в галузі інформаційної безпеки, зокрема антивірусів), за 2012 рік кількість хакерських атак збільшилася на 42%. Щодня системи інформаційної безпеки по всьому світу відображають близько 247 тисяч атак. У середньому кожен успішний злом дає хакерам доступ до особистих даних 604 інтернет-користувачів. За даними американського телеком-оператора Verizon, 75% хакерських атак виробляються з метою збагачення. Крім них, є ще «протестні» кібератаки - з політичним підґрунтям, з яких 75% - справа рук групи Anonymous.

За даними німецького оператора зв'язку Deutsche Telekom, Україна – на 4-му місці в світі після Росії, Тайваню та Німеччини серед країн, з яких в основному йдуть кібератаки. Щомісяця з українських серверів запускається понад півмільйона шкідливих програм.

Керівник відділу фінансової стабільності Банку Англії Ендрю Хелдейн заявляв, що найбільші 5 банків Великобританії бояться кіберзлочинів навіть дужче, ніж боргової кризи. За його словами, система захисту від хакерських атак у банківському секторі досі перебуває в зародковому стані: фінансисти більше дбали про ліквідність, аніж про безпеку. За експертними оцінками, щорічні втрати від шахрайства, зокрема, з банківськими картами в світі сягають 10-12 млрд. дол

Серед гучних атак у світі на фінансові структури за останні роки можна пригадати взлом сайтів MasterCard, Visa і Paypal групою Anonymous (кінець 2010-го), коли ті відмовилися приймати платежі для сайту WikiLeaks. Збиток від атаки склали 5,5 млн. дол. Пізніше люди, пов'язані з атакою, були арештовані і засуджені. Крім того, в червні 2011 р. сервери Citibank атакували хакери. Спочатку повідомлялося, що в руки зловмисників потрапили тільки імена, номери рахунків і контакти більш 360 тисяч вкладників. Пізніше керівництво Citigroup визнало, що хакери викрали 2,7 млн з рахунків 3400 клієнтів. Citibank обіцяв відшкодувати понесені клієнтами збитки.

Для протистояння кібершахраям в різних країнах створюються спецпідрозділи. Їхні повноваження постійно розширюють, а технічні можливості посилюють. Один з останніх прикладів – Європейський центр боротьби з кіберзлочинністю, який запрацював на початку 2013-го. Практично тоді ж у Росії президент В. Путін доручив ФСБ створити держсистему виявлення, попередження і ліквідації наслідків комп'ютерних атак на інформаційні ресурси країни.

Україна: банківський контекст кіберзлочинності

Основні способи кіберзлочинності в банківській сфері:

- *Скімінг* - установка спеціальних пристосувань, що зчитують дані карток на банкоматах або POS-терміналах (або замість POS-терміналів) в торгових точках.
- *Фішинг* - спроби виманити дані про картку через розсилку картодержателям електронних листів з проханням надати відповідну інформацію (типу: ви виграли приз чи в лотерею, отримали спадок і т.д., дайте дані про свій картковий рахунок, куди можна перерахувати гроші) або через відкриття «лівих» сайтів, де пропонується заповнити реквізити картки для отримання чогось.
- *Використання шкідливого програмного забезпечення* - більше стосується систем дистанційного обслуговування типу «клієнт-банк» (СДО), карткових рахунків відноситься у меншій мірі. Впровадження подібного ПО відбувається через електронну пошту або інтернет.
- *Злом банківських карткових систем* або систем передачі даних процесингових центрів.

За даними НБУ, у 2011 р. кількість протиправних операцій за банківськими картками підскочила до 7,6 тис. порівняно з 2,9 тис. роком раніше. Обсяг неправомірно списаних коштів збільшився майже в півтора рази - з 6,3 млн до 9,1 млн. грн. І це лише офіційна статистика (здебільшого банки намагаються відповідну інформацію не поширювати, щоб уникнути репутаційних втрат). У 2012 р. кількість махінацій з банківськими картками зросла на 47% - до 11,17 тисяч, а обсяг операцій збільшився на 20% - до 10,92 млн грн. (0,0015% від загального обсягу збитків банків).

Банкіри звертали увагу, що кіберзлочинці трохи послабили увагу до карткового сектора і переключилися на онлайн-системи дистанційного банківського обслуговування (ДБО), зокрема системи «клієнт-банк». Причому зменшується вплив одиночок і збільшується – організованих груп злочинців. «Якщо ще два роки тому це були поодинокі випадки, то в 2012 р. кількість і обсяг злодійських трансакцій зросли в рази. Найбільша склала 32 млн грн і була розбита на частини по 30 і 2 млн грн. Більшу трансакцію вдалося встановити тільки завдяки інструментам фінансового моніторингу НАБУ», - розповідав голова ради банківського об'єднання Борис Тимонькин. Додатково банкіри занепокоєні тим, що у 2013 р. зафіксовані випадки массового застосування проти банків (одночасно проти десяти і більше банків) розподілених кібератак на зовнішні сервіси типу "відмова в обслуговуванні" (DDos-атаки).

Як запевняли банкіри, несанкціонований доступ до систем ДБО в більшості випадків шахраї отримують з вини клієнтів. Шахраї виводять досить великі суми з рахунків юридичних осіб, після чого переводять їх по ланцюжку з фіктивних юридичних або фізичних осіб і знімають готівкою. По рахунках фізосіб шахрайство в системах ДБО незначне.Більшість крадіжок відбуваються після 17.00 в п'ятницю, а власники рахунків дізнаються про це лише в понеділок, коли шахрайська операція давно завершена і гроші перекочували через десяток рахунків.

За даними МВС, в 2012 р. правоохоронними органами встановлено 139 фактів втручання в роботу систем ДБО з метою крадіжки коштів. У результаті цих операцій з рахунків юросіб-клієнтів банків списано 116 млн грн, 75% з яких органи МВС змогли повернути власникам або заблокували за результатами слідчих дій. «Динаміка свідчить про зростання таких злочинів, оскільки тільки в І кварталі 2013 року вже зафіксовано 127 звернень, сума збитків склала 34,3 млн грн, з яких органами МВС заблоковано 60%, кошти повернуті 51 клієнтові», - повідомляв заступник начальника управління по боротьбі з кіберзлочинністю МВС Леонід Тимченко.

Як повідомлялося, Українська міжбанківська асоціація членів платіжних систем ЕМА зафіксувала більше шахрайських операцій на підставі даних з антіфрод-системи міжбанківського обміну інформацією Exchange-online. За підсумками І кварталу – 146 спроб несанкціонованих переказів. До органів МВС подано 56 заяв. Сума збитків - 20 млн грн, з яких 10,5 млн грн повернуто.

Начальник управління по боротьбі з кіберзлочинністю МВС Максим Литвинов повідомляв, що за І півріччя 2013-го в єдиний держреєстр досудових розслідувань внесено 1878 заяв, пов'язаних з дрібним шахрайством в Інтернеті – майже стільки ж, скільки за весь 2012 рік (понад 2 тис.). Лише за червень зареєстровано біля 600 заяв громадян про інтернет-шахрайства, які завдали збитків 8,5 млн грн. (3,27 млн грн. відшкодовано). МВС зафіксувало кілька випадків витоку персональної інформації користувачів при використанні загальновідомих електронних платіжних систем.

Приклади кібезлочинів:

- На початку листопада поточного року повідомлялося, що група хакерів змогла зламати платіжну систему одного з українських банків і перевести собі на рахунок 16 млн грн. За даними СБУ, для проведення операції група кібершахраїв готувалася 5 місяців.

Четверо українців під керівництвом 32-річного киянина відкрили фіктивне підприємство-«одноденку» і підписали з банком договір, щоб встановити термінал для безготівкових розрахунків. За допомогою POS-терміналу їм вдалося проникнути в платіжну систему банку і перерахувати 16 млн грн на рахунок одного з учасників групи.
Наприкінці жовтня СБУ затримала всіх чотирьох учасників при спробі зняти гроші в касі банку. Організатор групи і раніше займався хакерськими атаками на території України і РФ, підробляв платіжні карти і встановлював скімери на банкоматах.

- У квітні поточного року СБУ при взаємодії із ФСБ Росії припинила діяльність групи кібершахраїв, які через системи інтернет-банкінгу за останні п'ять років викрали понад 250 млн. дол. (шкода банкам України на суму понад 3 млн грн і фінансовим установам Росії - майже 8 млрд російських рублів).

Хакери створили вірус, який проникав у комп'ютери при скачуванні фотографій або перегляді відео в інтернет. Він отримував доступ до даних бухгалтерії, програми 1С, паролів і електронним ключам, після чого передавав їх шахраям. Шкідлива програма постійно модифікувалася, тому антивірусні засоби захисту її не ідентифікували. Після отримання даних злочинці якийсь час вивчали діяльність підприємства, потім від імені компанії формували електронні платежі на рахунки підставних фірм. Тільки в Україні від їхніх дій постраждало більше 30 компаній.
У групі налічувалося близько 20 осіб, середній вік яких від 25 до 30 років. Це були програмісти, які працювали віддалено в Києві, Запоріжжі, Львові, Херсоні та Одесі. Як правило, вони не знали один одного. Потім дані передавалися на головний сервер в Одесі, там же працював головний організатор - 28-річний громадянин Росії.

- Наприкінці жовтня співробітники МВС у фахівці управління по боротьбі з кіберзлочинністю МВС ліквідували злочинну групу з п'яти чоловік, яка обікрала дітей, що страждають онкологічними захворюваннями, на суму 360 тис. грн.

Підозрювані з оголошень в Інтернеті отримували особисті дані людей, які збирають гроші на лікування дітей. Вони виготовляли дублікати SIM-карт з номерами мобільних телефонів потерпілих, які були визначені як основні телефони для управління банківськими рахунками. Після цього шахраї телефонували в банк, представлялися іменами потерпілих, повідомляли оператору дані і здійснювали переказ грошей на інші рахунки, знімаючи їх потім у банкоматах.
Всі злочинці раніше судимі. Троє на момент вчинення злочину перебували в місцях позбавлення волі. Через шахрайства четверо дітей померли, не отримавши меддопомоги.

Що роблять для захисту себе та клієнтів банки?

Виконавчий директор НАБУ, голова правління Укргазбанку Сергій Мамедов розповідав, що 36% випадків шахрайства відбувається, коли людина сама дає інформацію шахраям, наприклад, по телефону або через інтернет, 20% випадків – при втраті платіжної картки, в інших – при підробці.

В Інтернет-асоціації України (ІнАУ) констатували, що банки часто самі економлять на способах інформаційного захисту. «Рівень захисту банківських платежів в країні недостатній, клієнтам обіцяють стовідсоткову безпеку, але це, як правило, залишається на словах , - зазначав член правління ІнАУ Іван Пєтухов. - Банкам слід регулярно оновлювати захист платіжних систем, залучати до цього високооплачуваних фахівців і пам'ятати, що хакери за рівнем підготовки на голову вище звичайних системних адміністраторів».

Координатор же комітету НАБУ з питань банківської інфраструктури та платіжних систем Володимир Єременко висловлював упевненість у тому, що в зломах винні не тільки банки. "Клієнт часто сам порушує правила користування системою дистанційного керування рахунком, користується інтернетом з комп'ютера , на якому встановлена ця система , тоді як він взагалі не повинен бути в мережі, а запускати його слід електронними ключами. Шахраї в основному зламують не комп'ютер, а мізки клієнтів», - зауважував В. Єременко.

Але свідченням, що в самих банках не все так гладко із безпекою в сфері ДБО, є інформація про злочинні дії щодо клієнтських грошей самих банківських службовців. Один з останніх гучних випадків – як співробітник одного з найбільших в Україні банків скопіював електронні ключі доступу до банківських рахунків клієнтів і викрав з них майже 8 млн грн. Наприкінці травня співробітники прикордонслужби затримали з підробленими документами двох колишніх менеджерів банку при спробі перетнути кордон з частиною викрадених з рахунків клієнтів коштів .

У рамках боротьби з кіберзлочинністю Незалежна асоціація банків Україна пропонувала/мала намір вжити кілька заходів (частина з них, власне, вже реалізована):

1. Створити єдину систему обміну інформації про випадки кіберзлочинів під егідою Національного банку України. Туди стікатимуться всі дані про такі порушення від

фінансово-кредитних установ. На їх основі даних можна створювати інформаційні бази з «чорними списками», наприклад, шкідливих програм та інструкції для реагування. Плюсом такої бази є знеособлення джерела інформації, що убезпечить банки від репутаційних та інших втрат, а отже, робить їх зацікавленими у тому, щоб «ділитися» цією конфіденційною інформацією з іншими. Не секрет, що зараз вони цього часто не роблять, тому статистка про даний вид злочину, м'яко кажучи, неповна. Банку часом легше «зам'яти» справу. Існування такої єдиної системи має кардинально змінити ситуацію.

2. Спільно з Національною академією МВС та Управлінням по боротьбі з кіберзлочинністю мало намір організувати курси навчання для працівників служб безпеки банків і пропонують подумати про сертифікацію таких фахівців. Це буде своєрідною гарантією професійного рівня банківських «безпечників».

3. Запустити сайт «Антикібер» (http://anticyber.com.ua/), який акумулюватиме максимальну кількість інформації прокіберзлочинність і буде орієнтований передусім на користувачів фінансових послуг. На сайті можна отримати практичні поради про те, як не стати жертвою кіберзлочинця і убезпечити свої гроші.

4. Удосконалювати аконодавство в галузі боротьби з кіберзлочинністю і виходити зі спільними пропозиціями на НБУ, який має право законодавчої ініціативи.

5. Активізувати співпрацю з Національним технічним університетом «Київська політехніка» для стимулювання створення інноваційних проектів в галузі IT-технологій, зокрема в галузі інформаційної і кібернетичної безпеки банків. Загальновідомий факт: попри катастрофічне падіння рівня технічної освіти в Україні, саме тут народжуються провідні IT-фахівці світу. На жаль, часто їхній талант йде саме в русло «кіберзлочинності». Чому не використати ці таланти для творення «добрих справ»?

Як захистити себе від шахрайства користувачам фінансових послуг?

Щоб убезпечити свої карткові розрахунки, в НАБУ радили клієнтам банків наступне:

1. Нікому не повідомляйте ПІН-код своєї картки.
2. Нікому не повідомляйте реквізити своєї картки. Не заповнюйте реквізити своєї картки на незрозумілих сайтах.
3. Не залишайте ніде свою картку без нагляду, особливо разом із записаним ПІН-кодом.
4. Не випускайте свою картку з поля зору в торгових точках.
5. Нікому не повідомляйте свої логін і пароль входу в систему інтернет-банкінгу.
6. Не користуйтеся карткою в підозрілих банкоматах, негайно повідомляйте в сервісну службу при виявленні дивних пристроїв.
7. Не ведіться на фішингові повідомлення про те, що ви нібито щось виграли чи отримали.
8. Обов'язково користуйтеся сервісом СМС-повідомлень.
9. Не тримайте всі свої кошти на одному картковому рахунку. Не використовуйте для повсякденних розрахунків картку з більшим лімітом. Заведіть кілька карток. Одну - з невеликим лімітом (наприклад, до 10 тис. грн.) Для щоденних розрахунків у супермаркеті, ресторані, сплати мобільним операторам, за комунальні послуги і т.д. Другу - з великим лімітом для одноразових великих платежів (машина, квартира, дача і т.д.). Третю - для подорожей. Четверту - для дружини з лімітом, який не шкода втратити і без кіберзлочинців.
10. Користуйтеся картками банків, які пропонують різні програми захисту від несанкціонованого списання (страхові, лояльності, гарантії і т.д.).

За словами експерта, для попередження шахрайств у системах ДБО необхідно дотримуватися таких базових правил. По-перше, слід використовувати тільки ліцензійне програмне забезпечення, оскільки неліцензійний софт може містити або відкривати "лазівки" для зчитування інформації з комп'ютера. Також необхідно використовувати антивіруси та мережеві екрани відомих виробників із регулярним автоматичним оновленням баз і перевіркою комп'ютера.

Експерти також не рекомендують використовувати комп'ютер системи "клієнт—банк" для будь-яких інших цілей, крім проведення операцій зі своїми рахунками, а також використовувати системи дистанційного управління комп'ютером. Вони також радять не виходити в систему "клієнт—банк" через "небезпечні" комп'ютери (наприклад в інтернет-кафе), не використовувати Wi-Fi-підключення, тим більше в публічних місцях. Як варіант можна застосовувати двофакторну аутентифікацію (наприклад, клієнт повинен надати USB-ключ або смарт-карту і ще ввести пароль) та впровадження систем моніторингу операцій ДБО на етапі здійснення платежу банківськими операціоністами.

При цьому бажано, щоб пароль містив не менш як 15 символів і змінювався не рідше ніж один раз на два місяці. Після звільнення відповідального співробітника, а також у разі зараження комп'ютера вірусами потрібно повністю міняти паролі, чистити кеш, перевіряти антивірусом усі системи "клієнт—банк", з якими він стикався.

Крім того, доцільно, щоб платіжні документи підписувалися двома ключами електронно-цифрового підпису (наприклад директора і бухгалтера), що зберігаються незалежно один від одного. Завдяки правилу "двох рук" варіант передачі електронного цифрового підпису, паролів та іншої інформації "з необережності" трапляється дуже рідко. Але якщо трапляється, то тільки тоді, коли такої "необережності" припустилися одночасно кілька людей. А це вже змова.

Щоб банку було легше захищати рахунки клієнтів, експерти радять користуватися системою фільтрації IP-адрес входу системи "клієнт—банк". Суть послуги в тому, що банк отримує точні IP-адреси, при підключенні з яких можливе проведення платежів. З решти адрес воно просто блокується. Крім того, доцільно підключити послугу СМС-інформування про платежі, якщо ця можливість надається банком.

Слід зауважити, що банкіри пропонують послугу з перевірки робочих місць клієнтів на предмет захищеності від хакерських вторгнень. Суть послуги полягає в тому, що банківські фахівці, використовуючи напрацьовані всередині установи системи захисту від фінансових кібершахраїв, забезпечують клієнту надійний рівень безпеки, який мінімізує втрати в майбутньому.

За її словами, банк, на відміну від зовнішніх провайдерів, має інформацію про "поведінку клієнта" в системі "клієнт—інтернет-банкінг", про характер і особливості шахрайських атак. Таким чином, банк може таргетовано формувати необхідні умови інформаційної безпеки на боці клієнтів і, відповідно, надавати клієнтам практичні рекомендації, а не теоретичні припущення. Наприклад з антивірусного програмного забезпечення, рівня безпеки налаштувань браузерів, поштових програм, зберігання секретних ключів і багатьох інших параметрів.

ДОВІДКО:

Кримінальна відповідальність за кіберзлочини в банківській сфері:

За *статтею 185* Кримінального кодексу України таємне викрадення чужого майна (крадіжка) карається штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк від вісімдесяти до двохсот сорока годин, або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або позбавленням волі на строк до трьох років. Крадіжка, вчинена в особливо великих розмірах або організованою групою, - карається позбавленням волі на строк від 7 до 12 років з конфіскацією майна.

У *статті 190* ККУ передбачено, що шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки, карається позбавленням волі на строк від трьох до восьми років.

За *статею 200* ККУ підробка документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, електронних грошей, а так само придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ, платіжних карток або їх використання чи збут, а також неправомірний випуск або використання електронних

грошей - карається штрафом від трьох до п'яти тисяч неоподатковуваних мінімумів доходів громадян. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються штрафом від п'яти до десяти тисяч неоподатковуваних мінімумів доходів громадян.

У *статті 231* ККУ визначено, що умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, - караються штрафом від 3 тисяч до 8 тисяч нмдг.

За *статтею 361* ККУ несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, - карається штрафом від шестисот до тисячі нмдг або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 2 років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких вчинено несанкціоноване втручання, які є власністю винної особи.

Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду (яка в 100 і більше разів перевищує нмдг), - караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Слід звернути увагу на те, що 17.01.2012 набрав чинності Закон України «Про внесення змін до деяких законодавчих актів України щодо гуманізації відповідальності за правопорушення у сфері господарської діяльності». Відтепер за вчинення злочинів, передбачених статтями 200 і 231 КК України, встановлено єдиний вид покарання - штраф.