

PRAWO I KOMPUTERY



Na pytania czytelników napływające na adres prawo@chip.pl odpowiada **RAFAŁ KORCZYŃSKI**, prawnik zajmujący się problemami prawa komputerowego, autor publikacji w specjalistycznej prasie prawniczej.

Odpowiedzialność banków w przypadku e-kradzieży jest większa, niż chcą one to przyznać

Strzeż się bankiera!

Gdy e-złodziej przechwyci numer naszej karty płatniczej i opróżni konto, nie okrada on prywatnej osoby, ale... instytucję finansową. To bank usiłuje przerzucić poniesione straty na klienta, czyli na nas. A czyni to bezprawnie.

Jerzy Naumann

■ W Polsce można zaobserwować rozszerzanie się przestępczości elektronicznej. Szereg interesujących wiadomości na ten temat zawartych w artykule pt. „Skok na wirtualne pieniądze” (patrz: CHIP 10/2001, 22) wypada uzupełnić kilkoma informacjami przydatnymi wtedy, gdy złodziej dobierze się do naszego konta.

Czyj jest ten „plastik”?

Warto pamiętać, że karta wydana nam przez bank – obojętnie, czy bankomatowa, debetowa czy kredytowa – nie jest wcale nasza. W potocznym języku tak często posługujemy się tym skrótem („zapłaciłem moją kartą”), że tracimy z pola widzenia fakt, iż karta wcale nie jest „nasza”, lecz stanowi własność „naszego” banku. Przez cały czas: od momentu wydania do chwili zniszczenia.

Przy przestępstwie tzw. skimmingu, a więc podrobienia karty drogą zeskanowania paska magnetycznego i powielenia go na innej plastikowej karcie,

dochodzi zatem do przestępstwa sfałszowania własności banku, nie naszej. Tylko część zapisanych na owym pasku informacji to dane osobowe. Cała reszta to cyfrowe kody przynależne do oprogramowania maszyn obsługujących bank i jego połączenia z centralą danego systemu rozliczeniowego (VISA, VISA Electron, American Express itd.).

Jakie to ma znaczenie, że „nasza” karta wcale nie jest nasza? W momencie skopiowania danych magnetycznych umieszczo-

nych na karcie pokrzywdzony wskutek tego przestępstwa staje się bank. Oczywiście? Po-

zornie. Każdy, kogo dotknie ten problem, przekona się, że banki bronią się rękoma i nogami od stania się w tych sprawach pokrzywdzonymi. Dlaczego? Ponieważ stąd już tylko krok do odpowiedzialności banku względem klienta, a więc

zwrotu zagarniętych przez złodzieja pieniędzy.

Kręta droga pieniądza

Podobnie rzecz się przedstawia z innym rodzajem kradzieży: sytuacją, gdy zostaniemy okradzeni z karty, za pomocą której złodziej dokona następnie zakupów.

Ponieważ i tu natkniemy się na

ucieczkę banku od

odpowiedzialności,

warto wiedzieć, jak

działa mechanizm ob-

rotu środkami podczas

transakcji (płatności) doko-

nanej kartą. Otóż

tylko pozornie

płacimy naszymi

pieniędzmi. W rze-

czywistości płacimy

pieniędzmi banku, które

są przelewane z rachunku

„naszego” banku na konto sprze-

dającego nam towar czy usługę.

W momencie realizowania tego

przelewu (a więc faktycznej za-

płaty) dochodzi do jednoczesne-

go zablokowania przez bank na

naszym rachunku równowartości



List do prawnika

Programy z gazet

PYTANIE: Czy jeśli kupuję czasopismo, do którego jest dołączona płyta CD z pełną wersją np. gry, to czy muszę przez cały czas przechowywać też i gazetę, aby móc legalnie korzystać z aplikacji? Przecież jeśli wyrzucę licencję na jakiś drogi program, to jest on już nielegalny. Czy podobnie jest z grami dołączanymi do pism?

Czytelnik

ODPOWIEDŹ: Nie ma prostej odpowiedzi na to pytanie. Wynika to między innymi stąd,

iż wydawnictwa podpisują różne umowy z autorami bądź dystrybutorami oprogramowania. Zatem może być tak, iż program traktowany będzie jako legalny tylko i wyłącznie wówczas, gdy użytkownik ma również papierowe wydanie danego czasopisma. Jednak w większości przypadków wystarczy mieć płytę, która była załączona do gazety. Elementem decydującym będzie tutaj umowa licencyjna bądź dystrybucyjna, z którą należy się zapoznać. Jeżeli nie znajdziemy tam żadnych dodatkowych

zastrzeżeń, to papierowe wydawnictwo można przekazać na makulaturę.

Co do wyrzucenia licencji zaś: nie zawsze powoduje to delegalizację używanego software'u. Elementem potwierdzającym posiadanie legalnego oprogramowania jest przede wszystkim licencja, ale wielokrotnie w przypadku jej utraty za dowód legalności służy faktura zakupu oprogramowania. Na jej podstawie można wystąpić do dystrybutora o duplikat licencji.

Rafał Korczyński



Interwencje

Internet przez 0-700?

Otrzymałem ostatnio rachunek telefoniczny z TP SA zaskoczył mnie: 158 jednostek za numer 0-700. Moja żona i ja nigdy nie dzwoniły pod ten numer. Poszedłem po billing i co się okazało: połączenia z 0-700 są wykonywane w tym samym czasie co modemowe z 0202122. Niektóre strony wykonują przekierowanie. Czyżby TP SA o tym nie wiedziała? A może jest to brak dbania o klienta na rzecz zarobku w układzie z podmiotami kryjącymi się za owymi stronami? Pani w Biurze Obsługi Klienta powiedziała mi, że „gdybym nie używał Internetu na czarno” (przecież numer 0-20 21 22 to usługa TP SA!), „tylko skorzystał z ich usług” (domyślam się, że chodzi o SDI lub ISDN), „tobym podobnych niespodzianek uniknął”. Poza tym dowiedziałem się, że „mogę zablokować prefiks 0-700 w moim telefonie – wystarczy o to poprosić” (taka usługa to TYLKO 3,66 zł

miesięcznie – kolejny zarobek). Jak widać, to, że nie wiedząc o istnieniu takich przekierowań, pozwoliłem sobie na nabicie jednostek przez 0-700, jest wyłącznie moją winą. Przecież TP nie musi nigdzie wspominać o takich rzeczach, bo i po co? Zarobek musi być.

Rafał Bronś

ODPOWIEDŹ

Telekomunikacja Polska SA oferuje dostęp do Internetu, jednak – podobnie jak inni operatorzy telekomunikacyjni – nie może ponosić odpowiedzialności za treści przekazywane za pośrednictwem Sieci czy oszustwa, których ofiarą może stać się internauta. Takim oszustwem jest przekierowywanie połączeń z numerami dostępowymi 0-20 na numery 0-700 lub na numery zagraniczne, z czym, niestety, spotykają się polscy internauci.

TP SA ostrzegała klientów przed takimi praktykami przede

wszystkim za pośrednictwem mediów. Nie jest jednak w stanie uchronić wszystkich przed podobnymi zdarzeniami. Wszyscy korzystający z Internetu powinni uważnie śledzić komunikaty pojawiające się podczas surfowania po Sieci, co



umożliwi uniknięcie przekierowania połączenia. Wyjściem z sytuacji jest też zablokowanie połączeń z numerami 0-700.

Michał Potocki

rzecznik prasowy TP SA

KOMENTARZ CHIP-A

Rzeczywiście, TP SA nie ponosi odpowiedzialności za działania oszustów wykorzystujących ich sieć telekomunikacyjną. Jednak każdy usługodawca (w tym wypadku firma oferująca usługi dostępne pod numerem 0-700) powinien w wyraźny sposób podać wysokość stawki za połączenie. Nie rozstrzygniętą sprawą jest, czy taki wymóg istnieje w odniesieniu do połączeń internetowych. W przypadku podstępnego przekierowania na 0-700 można próbować skarżyć firmę bez naszej wiedzy i zgody łączącą nas z własnym numerem dostępowym, choć skuteczność takiego postępowania nie jest pewna.

Z ciekawością natomiast dowiedzieliśmy się, że ktoś w mediach prowadził akcję informacyjną nt. zagrożeń związanych z przekierowywaniem połączeń z 0-20 na 0-700. Niczego takiego dotąd nie zauważyliśmy.

Rafał Korczyński

przelanej kwoty (na rzecz osoby trzeciej, u której dokonaliśmy zakupu). Dopiero po pewnym czasie nasz rachunek zostanie obciążony i bank odbierze zapłaconą za nas sumę. Jak długi to czas? Łatwo to sprawdzić, jeśli korzysta się z bankowości internetowej. Jeżeli dokonaliśmy ostatnio płatności kartą, z pewnością zauważymy, że saldo rachunku będzie wyższe niż limit dostępnych środków. Różnica to właśnie suma zablokowana do odprowadzenia z naszego rachunku na rachunek banku. Cały proces dobiega końca, gdy tylko zakończą się procedury weryfikujące transakcję.

Karta kredytowa jak sejf

Jaki z tych informacji płynie pożytek? Ano po pierwsze, uświadamia, jak ważne jest natychmiastowe powiadomienie banku lub instytucji weryfikującej

transakcje (Polcard, eCard), gdy tylko spostrzeżemy kradzież karty. Warto pieczołowicie odnotować czas zgłoszenia, upewniając się jednocześnie co do nazwiska pracownika, który odebrał informację. Nie od rzeczy będzie także powtórzenie zgłoszenia natychmiastowo wysłanym faksem, co da nam pisemne potwierdzenie daty i godziny poinformowania banku (raport faksu).

Kto tu jest ofiarą?

Ale ważniejszy jest pożytek drugi: to nie my zostaliśmy okradzeni, to znaczy – nie tylko my. Najpierw został okradziony bank. Nas nikt nie okradł, tylko nie możemy odzyskać od banku pieniędzy, które ten przeksięgował z naszego rachunku na swój. Nie dajmy się nabrać na zręcznie propagowane przez banki scenariusze! Z kradzieżą elektroniczną rzeczy mają się

bowiem od strony prawnej zupełnie tak jak ze zwykłą: gdy rabusie dokonają napadu na bank, kradnąc pieniądze – choćby i te konkretne banknoty, które dopiero co tam złożyliśmy, wpłacając na konto – okradną instytucję finansową, a nie nas! Jeżeli nasze pieniądze znalazły się po drugiej stronie okienka, to od tego momentu ryzyko związane z ich przechowaniem przeszło na bank. I bank, oczywiście, zwróci swoim klientom wszystkie skradzione podczas napadu środki. Jeśli nie dobrowolnie, to mocą wyroku sądowego. Niedawno miał miejsce ciekawy proces, gdy bank odmówił klientowi odszkodowania za depozyt wartościowy złożony w wynajętej skrytce. Bank przegrał, sąd nakazał wypłacenie odszkodowania klientowi.

Nie pozwalamy więc bankom na ucieczkę od odpowiedzialności za powierzone im

przez nas w depozyt środki! Nawet w pojedynkę nie jesteśmy bez szans! Oczywiście jeśli to nie my chcemy naciągnąć bank. Musimy jednak oprócz uczciwości zachować ostrożność w posługiwaniu się kartą i PIN-em. Obowiązuje nas regulamin wręczony nam wraz z kartą płatniczą. Przeczytajmy go uważnie, ale nie traktujmy jak obowiązujące prawo! To tylko umowa, a zatem podlega badaniu za pomocą rozmaitych procedur, m.in. sądowych. A w razie większej szkody – nigdy nie kapitulujemy. ■

Tytuł i śródtytuły pochodzą od redakcji.

INFO



Na CHIP-CD
w dziale
Porady | Prawo

znajduje się artykuł z CHIP-a 10/2001 na temat przestępstw popełnianych za pomocą kart płatniczych.