

## Skradną tożsamość i pieniądze

Rośnie liczba postępowań w sprawie przestępstw popełnionych w sieci

Sylwia Czubkowska  
Małgorzata Kryszkiewicz  
Iwona Łoboda  
dgpe@infop.pl

Wyludzenia tożsamości i informacji (tzw. phishing) oraz oszustwa w e-handlu – to największe plagi w polskim internecie. Liczba wszczętych postępowań w tych sprawach rośnie o kilkanaście procent rocznie.

W kwietniu klienci BZW BK, w sierpniu Deutsche Banku, a na początku września użytkownicy Allegro. Nie ma miesiąca, aby polskich internautów nie dotknął masowy atak phishingowy. Ten proceder polega na wyludzeniu takich danych, jak hasło do konta bankowego, PIN i numer karty kredytowej. Oszuści wykorzystują do tego spe-

cialnie spreparowane e-maile, a ostatnio SMS-y udające te wysyłane przez banki. Wzrost takich przestępstw widać w statystykach policji. Gdy w 1999 roku wszczęto 182 postępowania w związku z naruszeniem tajemnicy korespondencji (art. 262 k.k.) i 152 związane z ochroną danych osobowych, to w ubiegłym roku było

ich odpowiednio 1194 i 330. W I połowie tego roku wszczęto postępowanie w blisko 3,7 tys. takich spraw. A większość firm, których klientów dotyka phishing, woli się tym nie chwalić, nawet przed organami ścigania.

Na celowniku przestępców coraz powszechniej też znajdują się kupujący i sprzedający w sieci. – Prosta zasada:

handel sieciowy bardzo się spopularyzował. I oszuści to wykorzystują – mówi Zbigniew Engiel z laboratorium informatyki śledczej Media-recovery.

A Marek Bentkowski z Instytutu Informatyki Śledczej

Więcej na  
: [www.gazeta-prawna.pl/](http://www.gazeta-prawna.pl/)



ostrzega, że coraz częściej internetowi oszuści podszywają się pod kupujących i już na samym końcu procesu wykradają zamówione przedmioty. Stosują też inne, wyszukane sposoby: – Wysyłają spreparowany e-mail do kupującego, że wygrał aukcję. Podają w nim dane osoby, która faktycznie wystawiła towar, ale numer konta bankowego należy już do nich – opowiada Bentkowski.

A7 Życie gospodarcze kraj  
B10 Prawo

## Sieciowi oszuści atakują klientów na masową skalę

### Handel

Sylwia Czubkowska

sylwia.czubkowska@infor.pl

Tylko w pierwszych sześciu miesiącach policja wszczęła 3,7 tys. postępowań w związku z oszustwami internetowymi. Dziesięć lat temu przez cały rok było ich ledwie 577.

– Zamówiłam tabletki wspomagające odchudzanie od sprzedawcy, który reklamował się na jednym z portali ogłoszeniowych. Kosztowały blisko 600 zł. W paczce dostałam mydło – opowiada nam Kamila Krukowska z Warszawy. Jej przypadek nie jest odosobniony. Jak wynika z danych policji, przestępstwa internetowe są

coraz powszedniejsze, szczególnie te związane z handlem sieciowym.

Jeszcze kilka lat temu włamanie na serwery, wyludzenie danych czy oszustwa na aukcjach internetowych były sporadyczne i traktowane jako ciekawostki. W 1999 r. było ich łącznie zaledwie 380, w 2005 – 930. Tymczasem tylko w pierwszej połowie 2010 r. policja odnotowała 3700 podobnych przestępstw – dwuipółkrotnie więcej niż w tym samym okresie roku ubiegłego.

Coraz więcej skarg na sklepy internetowe napływa także do UOKiK. W zeszłym roku było ich 24 849, podczas gdy w 2009 – tylko około 18 tys. Przy tym

do urzędu konsumentów skarżą się nie tylko na oszustwa, lecz także na łamiące ich prawa regulaminy sklepów czy opóźnienia w dostawach.

– A to i tak tylko wierzchołek góry. Do policji trafia kilka razy więcej zgłoszeń, tyle że nie zawsze są wystarczające dowody o popełnieniu przestępstwa lub nie zawsze funkcjonariusze wiedzą, jak zabrać się do ich zbierania – mówi Zbigniew Engiel z laboratorium informatyki śledczej Mediarecovery.

Kamila Krukowska policjantom dostarczyła pełną korespondencję ze sprzedawcą, namiary na innych oszukanym i na samego sprzedawcę. – Na

policjantach jednak musiałam niemalże siłą wymóc, aby wydali oświadczenie o rozpoczęciu postępowania i aby poczta mogła wstrzymać przelew – dodaje.

– Ale obecnie świadomość policjantów w tym zakresie jest znacznie większa niż jeszcze kilka lat temu – zapewnia Engiel. Dodaje, że powszechność tych przestępstw powoduje, iż funkcjonariusze nie mogą się już uchylać od ich ścigania i coraz częściej przechodzą szkolenia z tego, jak walczyć z e-oszustwami.

### CZYTAJ TAKŻE

Uwaga na aukcje internetowe!  
[www.gazetaprawna.pl/biznes](http://www.gazetaprawna.pl/biznes)



# Zamiast upragnionej pracy dostaniesz kredyt do spłaty

Przestępcy zbierają informacje podczas **falszowych rekrutacji do pracy**. Przejmują także dane osobowe użytkowników portali aukcyjnych. Potem na ich konto biorą pożyczki

**Małgorzata Kryszkiewicz**  
**Iwona Łoboda**  
gp@infop.pl

Kilka dni temu na warszawską komendę policji Praga-Północ zgłosiły się osoby, którym skradziono tożsamość. Był to skutek fałszywej rekrutacji do pracy, przeprowadzonej przez przestępców. Osoby, które liczyły na zatrudnienie, wysłały listownie na adres podany w ogłoszeniu nie tylko swoje CV, ale także kserokopie dowodów osobistych. W ten prosty sposób przestępcy weszli w posiadanie danych kilkudziesięciu osób. Kiedy kandydaci do pracy stawili się pod adresem wskazanym w ogłoszeniu na rozmowę kwalifikacyjną, okazało się, że o ich przyszłym potencjalnym pracodawcy nikt nie słyszał. Policja ostrzega – taki sposób kradzieży tożsamości jest obecnie bardzo popularny wśród grup przestępczych. Falszywe ogłoszenia pojawiają się na osiedlowych tablicach ogłoszeń i w prasie. Jednak najczęściej oszuści łowią swoje ofiary za pośrednictwem internetu.

Takich problemów jest coraz więcej, ponieważ sieć daje nowe możliwości dotarcia do ludzi. Korzystając z tego narzędzia komunikacji trzeba być świadomym tego, że może ono być źródłem wielu zagrożeń – ostrzega Mariusz

Sokołowski, rzecznik prasowy Komendy Głównej Policji.

## Przetwarzanie danych

Opisany proceder stanowi przestępstwo, o jakim mowa w ustawie o ochronie danych osobowych. Zgodnie z jej art. 49 za przetwarzanie danych, do których przetwarzania osoba nie jest uprawniona, grozi kara grzywny, ograniczenia wolności bądź pozbawienia wolności do lat 2.

Nie ma tutaj znaczenia, co ta osoba zrobi ze zdobytymi w ten sposób informacjami. Wystarczy, że nie były one dla niej przeznaczone. Nawet jeżeli wsadzi je do szuflady i nie będzie ich dalej przekazywać, to i tak poniesie odpowiedzialność karną – tłumaczy Marian Filar, profesor z Uniwersytetu Mikołaja Kopernika w Toruniu.

Problem jednak polega na tym, że ciężko jest udowodnić popełnienie tego przestępstwa. Ponadto bardzo często sami poszkodowani nie zdają sobie sprawy z tego, że padli jego ofiarami, i nie zgłaszają tego na policję. Co gorsza, takie zgłoszenie i tak niewiele im pomoże.

Policja nie przekazuje informacji o podejrzeniu popełnienia przestępstwa kradzieży tożsamości innym instytucjom, takim jak np. banki – przyznaje asp. Monika Brodowska, oficer prasowy z komendy dla Warszawy Praga-Północ.

Może więc się okazać, że za kilka miesięcy osoba, której dane zdobyli przestępcy, otrzyma z banku wezwanie do zapłaty pierwszej raty rzekomo zaciągniętej przez nią pożyczki.

## Kradzież dokumentu

Osoba okradzona z tożsamości jest więc w nieciekawej sytuacji. To, że doszło do takiego przestępstwa, nie zostanie odnotowane w żadnej bazie czy urzędzie.

Zupełnie inaczej jest w sytuacji, gdy złodziej ukradł po prostu dokument tożsamości. Paradoksalnie ofiara takiego przestępstwa jest w lepszej sytuacji od tej, której skradziono jedynie dane. Kradzież dowodu osobistego można bowiem zgłosić do banku oraz zawiadomić o tym odpowiedni urząd gminy. Takie ruchy zablokują złodziejowi możliwość popełniania dalszych przestępstw przy użyciu skradzionego dowodu tożsamości.

Banki korzystają z systemu dokumentów zastrzeżonych.

W systemie można zastrzeżać tylko utratę dokumentu tożsamości – dowód, prawo jazdy albo paszport. Dzięki temu osoba, która padła ofiarą złodzieja, nie musi się już obawiać, że ktoś np. wyłudzi na jej konto kredyt – tłumaczy Iwona Słowik z Centrum Prawa Bankowego i Informacji.

## Jak się bronić przed kradzieżą tożsamości

### ➤ Zabezpiecz:

numery ubezpieczenia społecznego (SSN)  
karty kredytowe i debetowe  
numery PIN  
hasła do kont bankowych, portali aukcyjnych, kont internetowych

### ➤ Powiadom bank o:

podejrzanych telefonach, podczas których rozmówca prosi o podanie numeru konta w celu jego weryfikacji  
nieprawidłowościach zauważonych np. na wyciągach z kart kredytowych

### ➤ Skutecznie niszczyć zbędne dokumenty zawierające dane osobowe

### ➤ Nie odpowiadaj na e-mail z prośbą o podanie danych osobowych lub finansowych

### ➤ Nigdy nie wyrzucaj do śmieci dokumentów zawierających dane rachunkowe

### ➤ Logując się w internecie do konta bankowego, zawsze sprawdzaj, czy w pasku przeglądarki znajduje się ikona lock, jeżeli jej nie będzie – nie podawaj swoich danych

Dodaje, że oszust, który będzie próbował wziąć pożyczkę na dokument, który został zastrzeżony w bazie, zostanie od razu zatrzymany przez policję.

Niestety w bazie nie można zastrzeżać, że doszło do kradzieży tożsamości.

## Cele przestępców

Osobom, którym ukradziono tożsamość, pozostaje więc czujność. Jak tylko zauważą, że coś nie zgadza się np. w ich historii rachunku, powinny od razu zgłaszać to do swojego banku i próbować wyjaśnić sytuację. Należy bowiem pamiętać, że przestępcy zazwyczaj nie poprzestają na wyłudzeniu danych. Popołniają to przestępstwo, aby na konto swojej ofiary dopuszczać się dalszych czynów zabronionych.

Posługując się zdobytymi w nieuczciwy sposób danymi, oszuści mogą więc np. wyprodukować fałszywe dowody tożsamości, wyłudzać kredyty czy handlować fikcyjnymi przedmiotami na internetowych portalach aukcyjnych. Coraz częściej dochodzi także do wypożyczania samochodów oraz wynajmowania mieszkań, a osoba, której tożsamość skradziono, otrzymuje wezwanie do zapłaty kilkumiesięcznych zaległości w czynszu lub do zwrotu auta i uregulowania rachunku za jego wynajęcie.

## Wyłudzenie w internecie

Na utratę tożsamości szczególnie narażeni są internauci. Bardzo często padają oni ofiarami tzw. phishingu. Proceder ten polega na wyłudzeniu takich danych, jak np. hasło do witryny internetowej, numer karty kredytowej itp. Oszuści uzyskują takie informacje w ten sposób, że prezentują ofierze całą stronę bądź jej element do złudzenia przypominający oryginał. W ten sposób

niczego nieświadoma ofiara, myśląc, że loguje się do swojego banku, przesyła informacje przestępcy.

Ponadto cyberprzestępcy włamują się na konta allegrowiczów i sprzedają fikcyjne przedmioty. Za takie przestępstwo grozi kara od 6 miesięcy do 8 lat więzienia. Osoba, której skradziono tożsamość, powinna się szybko skontaktować z portalem.

Jeśli na portalu aukcyjnym dochodzi do kradzieży tożsamości, policja w pierwszej kolejności ustala, kto otrzymał pieniądze, czyli kto skorzystał na tej transakcji. Osoba, która włamuje się na cudze konto, najczęściej sprzedaje fikcyjne przedmioty, by łatwo i szybko zarobić – tłumaczy Marek Bentkowski z Instytutu Informatyki Śledczej.

Co ciekawe, kradzież tożsamości na Allegro może dotyczyć nie tylko sprzedających, ale również kupujących.

Zajmowałem się kiedyś sprawą zaginięcia telefonu komórkowego. Policja w pierwszej kolejności odwołała się do sprzedawcy przez internet. Okazało się jednak, że sprzedający wyłudził się ze swoich obowiązków. Osoba, która wygrała licytację, również wysłała pieniądze, ale ślad po telefonie zaginął. Nie wiadomo, kto go odebrał – opowiada Marek Bentkowski.

I ostrzega, że bywają także przypadki, w których internetowi oszuści wysyłają spreparowanego e-maila do kupujących z informacją, że wygrali aukcję. Podają w nim dane osoby, która faktycznie brała udział w licytacji, ale numer konta bankowego należy już do nich. Ofiarami takich przestępstw zostają najczęściej osoby, które logują się z różnych komputerów, gdzie zostawiają swoje dane.

## trzy pytania



**RAFAŁ WIEWIÓROWSKI**  
generalny inspektor danych osobowych

**Czy do GODO docierają sygnały o próbie wyłudzenia danych osobowych pod pozorem rekrutacji do pracy? Jakiego kroki może wówczas podjąć?**

Do GODO docierają sygnały o próbie wyłudzenia danych osobowych, przy czym sposoby i cele wyłudzenia danych bywają różne. Czasami dane pozyskiwane są na potrzeby budowy osobnej bazy danych, a czasami wręcz w celach przestępczych. GODO może podjąć działania na przykład wówczas, gdy przedsiębiorca (pracodawca) pozyskuje dane osobowe pod pozorem prowadzenia rekrutacji, a następnie wykorzystuje je do innych celów, np. marketingowych. Bowiem GODO – stosownie do zakresu jego zadań określonego w art. 12 ustawy o ochronie danych osobowych – kontroluje zgodność przetwarzania danych osobowych z przepisami o ich ochronie oraz rozpatruje skargi w sprawach wykonywania tych przepisów. GODO może wszcząć postępowanie administracyjne na skutek skargi albo z urzędu, zaś po przeprowadzeniu postępowania w sprawie i ustaleniu wszystkich zaistniałych okoliczności wydaje stosownej treści decyzje administracyjne nakazujące administratorowi danych przywrócenie stanu zgodnego z prawem w razie stwierdzenia, iż dane przetwarzane są z naruszeniem przepisów o ich ochronie.

**A co w sytuacji, gdy GODO stwierdzi, że wyłudzone dane w celach przestępczych?**

Jeśli w toku prowadzonych działań GODO stwierdzi, że działanie lub zaniechanie danego podmiotu będącego administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie o ochronie danych osobowych, to do organów ścigania kieruje zawiadomienie o popełnieniu przestępstwa, dołączając na to dowody (art. 19 ustawy o ochronie danych osobowych).

**Czy wyłudzenie danych osobowych można uznać za stalking?**

O ile dane osób, które odpowiadają na ogłoszenie rekrutacyjne, są wykorzystywane przez kogoś, kto je pozyskał, do uporczywych kontaktów (co się zdarza, jak wynika z sygnałami docierającymi do GODO), opisaną sprawę należałoby rozpatrywać w kontekście przestępstwa tzw. stalkingu, o którym mowa w art. 190a ustawy – Kodeks karny. Zgodnie z tym przepisem kto przez uporczywie nęka inną osobę lub osobę jej najbliższą, wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności do lat 3. Tej samej karze podlega, kto podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej. Ściganie takich przestępstw następuje na wniosek pokrzywdzonego. W związku z tym osoba pokrzywdzona powinna zgłosić sprawę do organów ścigania (policja, prokuratura). W takich bowiem sprawach chodzi przede wszystkim o ustalenie sprawcy przestępstwa, a uprawnione do tego są tylko organy ścigania.

Rozmawiała Małgorzata Kryszkiewicz