

## ***Prawno-kryminalistyczna problematyka phishingu, ze szczególnym uwzględnieniem środowiska bankowości internetowej***

Daniel Lubowiecki

---

Termin „phishing” powstał w połowie lat 90. XX w. Po raz pierwszy posłużono się nim na łamach hakerskiego magazynu „2600”. Określenie to przeważnie tłumaczy się, jako *password harvesting fishing* (ang. łowienie haseł), można spotkać się też z opinią, że powstało ono poprzez połączenie słów *fishing* (ang. rybołówstwo) oraz *phreaking* (ang. łamanie zabezpieczeń komputerowych)<sup>98</sup>. Jest to rodzaj oszustwa, polegający na podszywaniu się przez sprawcę pod inną osobę lub organizację, w celu wyłudzenia określonych informacji (np. danych logowania do bankowości internetowej) lub nakłonienia ofiary do realizacji określonych działań<sup>99</sup>.

Phishing, nazywany jest niekiedy „nową kategorią cyberprzestępczości XXI wieku”<sup>100</sup>. Warto zauważyć jednak, że nie jest to nowe zjawisko a pierwszy atak phishingowy na dużą skalę odnotowano już w 1995 r. Sprawcy udając pracowników America Online (dalej: AOL)<sup>101</sup>, wysyłali wiadomości e-mail z prośbą o podanie hasła do konta. Jako argumentację podawali konieczność weryfikacji konta albo potwierdzenia danych na rachunku. Mając już tę informację, wkradali się na konta i spisywali dane kart kredytowych, które następnie wykorzystywali do własnych celów. Pomimo, że społeczność posługująca się AOL była informowana o potencjalnym zagrożeniu komunikatem o treści „Żaden pracownik AOL nigdy nie zapyta o twoje hasło lub dane do opłacenia rachunku”, liczba poszkodowanych stale rosła<sup>102</sup>.

---

<sup>98</sup> R. Janus, M. Delio, *Niebezpieczne wędkowanie*, „PC World Komputer” nr 04/2005, Warszawa 2005, s. 148.

<sup>99</sup> M. Górniewicz, R. Obczyński, M. Pstruś, *Bezpieczeństwo finansowe w bankowości elektronicznej-przestępstwa finansowe związane z bankowością elektroniczną*, Warszawa 2014, s. 7.

<sup>100</sup> J. Nawrat, *Phishing i antyphishing w bankowości internetowej*, „Boston IT Security Review” nr 4, 2008, s.50.

<sup>101</sup> America Online jest jednym z głównych dostawców usług internetowych. Powstał w 1983 roku jako Quantum Computer Services, w późniejszych czasach posługiwał się nazwą America Online. W latach 90. AOL był utożsamiany przez wielu Amerykanów z Internetem. W najlepszych latach obsługiwał ok. 30 milionów subskrybentów.

<sup>102</sup> M. Gajewski, *Phishing-łowienie naiwnych*, <http://www.chip.pl/artykuly/trendy/2009/11/phishing-lowienie-naiwnych>, 06.11.2016.

Łatwowierność i naiwność użytkowników Internetu sprzyja cyberprzestępcom posługującym się inżynierią społeczną. Kolejnym atakiem na dużą skalę było wyłudzenie danych osobowych od klientów instytucji E-gold<sup>103</sup>. Tym razem phisherzy wykorzystując lęk społeczeństwa spowodowany atakami na World Trade Center w Nowym Jorku z 11 września 2001 r. zgłosili się do jego klientów z żądaniem niezwłocznego potwierdzenia swoich danych personalnych. Argumentowali to koniecznością ochrony ekonomii kraju w związku z możliwą wojną na terenie Stanów Zjednoczonych. W tym przypadku liczba osób, które wpadły w pułapkę również była znaczna<sup>104</sup>.

Powyższe przykłady pokazują, że ataki phishingowe nie polegają jedynie na omijaniu zabezpieczeń komputerowych, ale przede wszystkim bazują na ludzkiej nieostrożności i łatwowierności.

Obecnie ataki phishingowe przybrały niewyobrażalnie wielką skalę. Według niektórych szacunków każdego miesiąca na całym świecie rozsyłanych jest ponad 6 miliardów e-maili próbujących wykorzystać phishing<sup>105</sup>. Tylko w 2014 r. CERT Polska zarejestrował ponad 85 tysięcy zgłoszeń phishingu dotyczących prawie 19 tysięcy adresów URL<sup>106</sup>. Należy podkreślić jednak, że statystyki te dotyczą tylko stron hostowanych w Polsce, a więc nie uwzględniają phishingów polskich instytucji, które hostowane były za granicą.

Pomimo ogromnej skali zjawiska, literatura poruszająca omawiane kwestie jest bardzo uboga. Niniejszy artykuł ma na celu ukazanie prawno-kryminalistycznej analizy problematyki phishingu, ze szczególnym uwzględnieniem środowiska bankowości internetowej, bowiem w tym obszarze w ostatnich latach skala zjawiska przybrała niespotykane dotąd rozmiary.

## Metody działania sprawców phishingu

Ataki phishingowe można podzielić ze względu na cel w który zostały wymierzone na:

1. masowe, czyli skierowany do jak najszerszego kręgu odbiorców,
2. grupowe, a więc wymierzone np. w klientów określonego banku lub innej instytucji,
3. spersonalizowane, czyli nakierowane na konkretną osobę.

<sup>103</sup> J. Gąsiorowski, P. Podsiedlik, *Przestępstwa w bankowości elektronicznej w Polsce. Próba oceny z perspektywy prawno-kryminalistycznej*, Dąbrowa Górnicza 2015, s. 146.

<sup>104</sup> Tamże.

<sup>105</sup> [www.sonicwall.com/fuhrl/phishing](http://www.sonicwall.com/fuhrl/phishing), 07.11.2016.

<sup>106</sup> Zespół CERT Polska działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) – instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty. W 2010 roku CERT Polska dołączył do Anti-Phishing Working Group, czyli stowarzyszenia gromadzącego firmy i instytucje aktywnie walczące z przestępczością w sieci.

Metody działania w każdym z wymienionych przypadków będą się od siebie różniły<sup>107</sup>.

Najpowszechniejsza forma phishingu polega na przesłaniu e-maili do potencjalnych ofiar, w których atakujący podszywa się pod zaufaną osobę lub instytucję. Jeżeli celem ataku są np. klienci konkretnego banku, to wiadomość spreparowana jest w taki sposób, aby łudząco przypominała korespondencje faktycznie wysyłaną przez jego pracowników. Wiadomość taka zawiera przeważnie informacje o anulowaniu transakcji, zablokowaniu konta lub o rzekomej próbie włamania się na nie przez osoby postronne a także wskazuje, że jedynym rozwiązaniem jest weryfikacja właściciela poprzez stronę internetową banku, do której odnośnik zostaje umieszczony w wiadomości.

W lutym 2016 roku klienci mBanku otrzymali wiadomość następującej treści:

### Rysunek. 1 Wiadomość wysłana do klientów mBanku



Źródło: <https://niebezpiecznik.pl/post/uwaga-klienci-mbanku/> (dostęp: 06.11.2016).

<sup>107</sup> W doktrynie można spotkać się również z innym podziałem rodzajów ataków phishingowych. F. Randoniewicz wśród nich wskazuje: a) *spear phishing*, który występuje, gdy e-maile sprawcy skierowane są do określonego kręgu podmiotów, b) *whaling*, gdy celem ataku są członkowie organów przedsiębiorstw, c) *social phishing*, czyli phishing, w którym środowiskiem działania sprawcy są portale społecznościowe. Zob. szerzej: F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 95-96.

Wiadomość z pozoru nie budziła żadnych podejrzeń, jednak po kliknięciu w zamieszczony link następowało przekierowanie na stronę [www.m-autoryzacja.com](http://www.m-autoryzacja.com), która została utworzona na potrzeby ataku. Jeżeli ofiara tego nie zauważyła i wpisała swój identyfikator oraz hasło została przekierowana na następną stronę, na której z kolei została poproszona o podanie numeru karty i jej ważności oraz kodu służącego do weryfikacji. Po wykonaniu powyższych czynności ofiara zostaje przekierowana na oficjalną stronę banku a podane informacje przesłane do phishera a następnie wykorzystane w przestępczym celu.

Aby link do strony nie budził podejrzeń phisherzy stosują różne techniki mające uspić czujność ofiary. Jedną z nich jest maskowanie adresu strony internetowej. Polega ono na tworzeniu domeny o bardzo podobnej nazwie do tej, której użytkownicy mają być celem ataku. Przykładowo, jeżeli strona internetowa banku dostępna jest pod adresem <https://www.bankxyz.pl>, to stworzona na potrzeby ataku domena może przybrać postać <https://www.bankxyz.com.pl>, <https://www.bankyxz.pl> czy też <https://www.bank-xyz.pl>. Popularnym sposobem jest także podmiana podobnych do siebie znaków jak np. „l” na „1” albo wykorzystanie IDN, czyli domen zawierających znaki spoza ASCII<sup>108</sup>. W tym przypadku adres URL banku mógłby wyglądać następująco: <https://www.bankxyz.com.pl><sup>109</sup>.

Kolejną techniką jest wykorzystywanie odsyłacza internetowego zapisanego w języku HTML, dzięki czemu pomimo, że w wiadomości widoczny będzie adres <https://www.bankxyz.pl> to faktycznie nastąpi przekierowanie na dowolną, wskazaną w odsyłaczu stronę<sup>110</sup>. Co prawda większość przeglądarek wyświetla na dole interfejsu adres do którego ma nastąpić przekierowanie, lecz niewielu użytkowników zwraca na to uwagę. Strony phishingowe często korzystają także z zakupionych albo przechwyconych z serwera innej strony certyfikatów SSL, co dodatkowo umacnia ich wiarygodność<sup>111</sup>.

Inna forma ataku phishingowego polega na przesłaniu wiadomości email z zainfekowanym załącznikiem np. pod pretekstem przesłania faktury. Pod koniec 2014 r. wielu klientów sieci Play otrzymało informacje o rzekomo nieuregulowanej płatności o treści:

<sup>108</sup> IDN (Internationalized Domain Name) jest to rodzaj domeny umożliwiający tworzenie adresów URL z wykorzystaniem znaków innych niż występujących w alfabecie łacińskim (ASCII) np. pochodzących z cyrylicy.

<sup>109</sup> Z pozoru identycznie wyglądający adres URL zostanie odmiennie zakodowany w Unicode. Zamiast łacińskiego „a” (o kod: U+0061) użyto znaku „a” z cyrylicy (kod: U+0430).

<sup>110</sup> Budowa odsyłacza HTML do adresu internetowego wygląda następująco: `<a href="adres internetowy">opis odsyłacza</a>`. Opis może być konstruowany dowolnie, może przybrać postać adresu innej strony albo np. polecenia „kliknij tutaj”.

<sup>111</sup> Certyfikaty SSL są narzędziem zapewniającym ochronę stron internetowych oraz gwarantem zachowania poufności danych przesyłanych drogą elektroniczną. Certyfikaty SSL są rejestrowane na określonej nazwę domeny, zawierają informacje o właścicielu domeny, jego adresie itp.

## Rysunek. 2 wiadomość wysłana do klientów sieci Play



Witaj, Krzysztof

Przypominamy o nieuregulowanej płatności za fakturę o numerze F/2853316/10/14 wystawioną w dniu 19/10/2014. Faktura w formie elektronicznej została dołączona do wiadomości. Jak czytać fakturę? - **instrukcja**.

|                          |                                                                    |
|--------------------------|--------------------------------------------------------------------|
| Forma płatności:         | <b>Przelew / Foto wpłata</b>                                       |
| Termin płatności:        | <b>31/10/2014</b>                                                  |
| Nazwa wystawcy:          | P4 sp. z o.o.<br>ul. Taśmowa 7, 02-677 Warszawa, NIP 951-21-20-077 |
| Kwota do zapłaty         | <b>331,27 zł</b>                                                   |
| Numer konta:             | <b>46 1090 0004 7777 0100 2573 5659</b>                            |
| Zalecany tytuł przelewu: | <b>Play faktura F/20249758/09/14 klient 25735659</b>               |

Dziękujemy za terminowe dokonywanie płatności, które chroni przed naliczaniem odsetek ustawowych.

Jednocześnie informujemy, że archiwum e-faktur znajduje się na serwisie **Play24**, gdzie można sprawdzić integralność treści i autentyczność pochodzenia załączonej faktury.

Zachęcamy do wypełnienia ankiety na temat e-faktury. Ankieta dostępna jest po zalogowaniu do Play24, w zakładce Faktury. Państwa opinia jest dla nas bardzo ważna. Dziękujemy!

Pozdrawiamy.

Wiadomość wysłana przez Spółkę P4 sp. z o.o., z siedzibą i adresem w Warszawie, ul. Taśmowa 7, 02-677 Warszawa, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000217207, prowadzonego przez Sąd Rejonowy dla miasta stołecznego Warszawy, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, NIP 951-21-20-077, REGON 015808609, ZSEE E0008436W, której kapitał zakładowy wynosi: 48 456 500,00 zł.

Źródło: <https://niebezpiecznik.pl/post/uwaga-na-falszywe-faktury-z-play/> (dostęp: 06.011.2016).

Jak widać, odbiorcy wiadomości adresowani byli imieniem i nazwiskiem co dodatkowo wzbudzało wrażenie autentyczności maili. Załączony w wiadomościach plik opisany został pod nazwą faktury z rozszerzeniem .pdf. Tak naprawdę człon „pdf” stanowił jedynie część nazwy pod którą zapisany został plik. Faktycznie było to rozszerzenie .pif. Jest ono najczęściej wykorzystywane w tego typu atakach, ponieważ jest zdolne do obsługi plików wykonywalnych a jednocześnie nie jest wyświetlane użytkownikom. Otwarcie takiego załącznika powoduje instalację na komputerze wirusa o nazwie *banatrix*, który podmienia ciąg liczb odpowiadający rachunkowi bankowemu na numer konta słupa<sup>112</sup>. Osobie dokonującej przelewu ciągle wyświetla się jednak poprawny nr konta. Co więcej, nawet po wejściu w historię operacji widnieje prawidłowy numer, dopiero po wydrukowaniu potwierdzenia ukazuje się numer na który faktycznie zostały przelane pieniądze. Jedynym sposobem weryfikacji, czy przelew trafi na właściwe konto jest sprawdzenie ostatnich czterech cyfr w wiadomości sms będącej

<sup>112</sup> Określenie „słup” oznacza osobę fizyczną, wykorzystaną przez przestępców podczas dokonywania różnego rodzaju oszustw w celu ukrycia faktycznego sprawcy czynu. Jest to określenie powszechnie stosowane przez kryminologów. Według definicji zawartej w Wielkim słowniku języka polskiego przez pojęcie „słupa” należy rozumieć osobę, która firmuje swoim nazwiskiem jakieś działanie, w celu ukrycia faktycznego inspiratora lub uczestnika.

narzędziem autoryzacyjnym (pod warunkiem, że sprawca nie przejął kontroli również nad telefonem).

Najbardziej wysublimowaną i najtrudniejszą do wykrycia formą ataku phishingowego jest tzw. *pharming*. Polega on na takim manipulowaniu „pytań o kierunek” zgłaszanych przez komputer, aby nastąpiło dyskretne przekierowanie użytkownika do fałszywej witryny stworzonej przez sprawcę. Można to osiągnąć poprzez ingerencję w pamięć podręczną DNS (*Domain Name System*) komputera lokalnego albo nawet całego serwera<sup>113</sup>. Oznacza to, że nawet jeżeli użytkownik ręcznie wpisze prawidłowy adres witryny to i tak zostanie przekierowany do strony phishingowej, pomimo, że na pasku przeglądarki nadal będzie wyświetlany prawidłowy adres.

### **Prawnokarna kwalifikacja phishingu**

Prawnokarna kwalifikacja phishingu jest zagadnieniem problematycznym i złożonym, ponieważ działania sprawców phishingu poprzez swoją różnorodność nie dają się przypisać do konkretnego przepisu karnego. Polskie prawo karne nie zna bowiem przestępstwa phishingu. Wskazać należy jednak, że działania polegające na podszywaniu się pod zaufaną osobę lub instytucję w celu wyłudzenia określonych danych osobowych wypełniają znamiona przestępstwa określonego w art. 190a § 2 k.k.<sup>114</sup>. Przepis ten stanowi, że karze pozbawienia wolności do lat 3 podlega ten, kto podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej. Przez podszycie się należy rozumieć przede wszystkim wprowadzenie w błąd innych osób co do własnej tożsamości. Z kolei za dane osobowe uznaje się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej w celu ustalenia jej tożsamości<sup>115</sup>.

Przestępstwo stypizowane w art. 190a § 2 k.k. ma charakter powszechny, formalny i może być popełnione jedynie w zamiarze kierunkowym<sup>116</sup>. Oznacza to, że zostaje dokonane już w momencie podszycia się za ofiarę tego przestępstwa przez sprawcę wykorzystującego jej wizerunek oraz dane osobowe. Ponadto, czynności sprawcze muszą być podjęte w celu wyrządzenia pokrzywdzonemu szkody majątkowej lub osobistej. W doktrynie podkreśla się,

---

<sup>113</sup> Zob. szerzej nt. DNS: *jak działa system DNS*, <https://www.kei.pl/blog/czyli-wiecej-o-systemie-dns/>, 01.01.2016.

<sup>114</sup> Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny, Dz.U. 1997 nr 88 poz. 553.

<sup>115</sup> S. Hypś [w:] Kodeks karny. Komentarz., red. A. Grześkowiak, K. Wiak, Warszawa 2014, s. 740.

<sup>116</sup> M. Mozgawa [w:] Kodeks Karny. Komentarz, red. M. Mozgawa, Warszawa 2014, s. 473.

że do jego dokonania nie jest potrzebne rzeczywiste spowodowanie szkody, wystarczy jedynie, aby sprawca dążył w tym kierunku<sup>117</sup>. W związku z tym, działania sprawcy phishingu polegające na stworzeniu fałszywej strony internetowej oraz zdobyciu w ten sposób danych potrzebnych do zalogowania się np. na witrynie banku oraz narzędzi autoryzacyjnych służących do wykonania przelewu wypełniają znamiona określone w art. 190a § 2 k.k., chociażby sprawca nie uzyskał w ten sposób korzyści majątkowej.

Uzyskanie danych osobowych na potrzeby ataku phishingowego może być następstwem tzw. przestępstwa komputerowego o którym mowa w art. 287 k.k. W myśl tego przepisu, kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do 5 lat. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Przestępstwo to może zostać popełnione na dwa sposoby. Pierwszy z nich polega na wpłynięciu bez upoważnienia na przetwarzanie, gromadzenie lub przekazywanie danych informatycznych<sup>118</sup>. Drugi zaś wiąże się z wpłynięciem na istniejące informacje. Może ono polegać na zmianie lub usunięciu danych istniejących w systemie informatycznym lub przybrać postać wprowadzenia nowych danych do systemu informatycznego. W tym przypadku jednak, sprawcy musi towarzyszyć określony cel, jakim jest chęć osiągnięcia korzyści majątkowej lub wyrządzenie szkody majątkowej innej osobie. Warunek ten sprawia, że przepis art. 287 k.k. jest przepisem szczególnym do innych przepisów karnych chroniących informacje<sup>119</sup>. Jak podkreślił Sąd Apelacyjny w Szczecinie w wyroku z dnia 14 października 2008 r. „Przestępstwo z art. 287 § 1 k.k., dokonane jest już z chwilą wprowadzenia zmian lub innej opisywanej w tym przepisie ingerencji w urządzenie lub system do gromadzenia, przetwarzania lub przesyłania informacji za pomocą techniki komputerowej. Efektywna szkoda nie należy zatem do jego znamion”. Podobnie zatem jak w art. 190a § 2 k.k., sprawca nie musi uzyskać korzyści majątkowej, aby jego zachowanie wypełniało znamiona omawianego przepisu.

<sup>117</sup> M. Filar [w:] Kodeks Karny. Komentarz, red. M. Filar i in., Warszawa 2016, s. 1174.

<sup>118</sup> Przez dane informatyczne należy rozumieć dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie informatycznym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny (art. 1b Konwencji o cyberprzestępczości sporządzonej w Budapeszcie dnia 23 listopada 2001 r.).

<sup>119</sup> T. Oczkowski [w:] Kodeks karny. Komentarz, red. Ryszard A. Stefański, s. 1701.

Jeżeli którekolwiek z wyżej wymienionych ingerencji poprzedza przełamanie lub ominięcie szczególnego zabezpieczenia danych informatycznych, sprawca phishingu dopuszcza się również czynu określonego w art. 267 k.k., który może być uznany za czyn współukarany uprzedni lub fragment czynu ciągłego<sup>120</sup>. W rozumieniu tego przepisu osoba bezprawnie uzyskująca dostęp do informacji dla niej nieprzeznaczonej, otwierająca zamknięte pismo, podłączająca się do sieci telekomunikacyjnej lub przełamująca albo omijająca elektroniczne, magnetyczne, informatyczne czy też inne szczególne jej zabezpieczenia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Tej samej karze podlega również ten, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego, jak również osoba, która w celu uzyskania informacji, do której nie jest uprawniona, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Penalizowane jest ponadto ujawnienie innej osobie informacji uzyskanych w ten sposób.

Dobrem chronionym tego przepisu jest więc przede wszystkim zabezpieczenie informacji przed dostępem ze strony osób nieuprawnionych. Aktualne brzmienie art. 267 k.k. umożliwia przypisanie odpowiedzialności karnej, nie tylko gdy sprawca zapoznał się z informacją nieprzeznaczoną dla niego, lecz także gdy przejął władztwo nad nośnikiem informacji. Z kolei znamień uzyskania dostępu do systemu informatycznego może obejmować zarówno część, jak i całość systemu<sup>121</sup>.

### **Odpowiedzialność banku za nieautoryzowaną transakcję będącą skutkiem ataku phishingowego**

Zgodnie z artykułem 725 k.c. przez umowę rachunku bankowego, bank zobowiązuje się względem posiadacza rachunku, na czas oznaczony lub nieoznaczony, do przechowywania jego środków pieniężnych, oraz jeżeli umowa tak stanowi, do przeprowadzania na jego zlecenie rozliczeń pieniężnych<sup>122</sup>. Zasady świadczenia tych usług oraz wydawania i wykupu pieniądza elektronicznego, w tym prawa i obowiązki stron wynikające z umowy o świadczenie usług

<sup>120</sup> M. Gałązka [w:] Kodeks karny. Komentarz, red. A. Grześkowiak, K. Wiak, Warszawa 2015, s. 1305.

<sup>121</sup> Zgodnie z art. 2 pkt 6 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. 2010 nr 182 poz. 1228, przez „system informatyczny” należy rozumieć zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy – Prawo telekomunikacyjne (Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz.U. 2004 nr 171 poz. 1800).

<sup>122</sup> Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny, Dz.U. 1964 nr 16 poz. 93.

płatniczych, a także zakres odpowiedzialności określone zostały w ustawie z dnia 19 sierpnia 2011 r. o usługach płatniczych (dalej: u.u.p.)<sup>123</sup>.

Bank krajowy w świetle w/w ustawy jest dostawcą usług płatniczych, co oznacza, że obowiązany jest m. in. do zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z niego (art. 43 ust. 1 u.u.p.)<sup>124</sup>. Użytkownik uprawniony do posługiwania się instrumentem płatniczym obowiązany jest z kolei do korzystania z niego zgodnie z umową ramową oraz nieudostępniania go osobom nieuprawnionym a także do zgłaszania niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia tegoż instrumentu lub nieuprawnionego dostępu do niego (art. 42 u.u.p.).

W przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca obowiązany jest niezwłocznie zwrócić płatnikowi utraconą kwotę, a jeśli korzysta on z rachunku płatniczego, przywrócić także obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca owa transakcja. Przez autoryzację transakcji należy rozumieć wyrażenie zgody na jej przeprowadzenie, czyli złożenie oświadczenia woli użytkownika z zamiarem i świadomością dokonania transakcji płatniczej. Sposób wyrażenia zgody powinien zostać określony w umowie zawartej pomiędzy dostawcą a płatnikiem<sup>125</sup>. Jeżeli autoryzacja następuje z wykorzystaniem instrumentu płatniczego, jego rodzaj oraz sposób używania powinien być również określony w umowie. W przypadku natomiast umów ramowych, sposób w jaki ma nastąpić autoryzacja transakcji, jest przeważnie określony w regulaminie dołączonym do umowy ramowej, stanowiąc jej integralną część<sup>126</sup>.

W razie naruszenia przez płatnika obowiązków związanych z zabezpieczeniem dostępu do instrumentu płatniczego odpowiada on za nieautoryzowane transakcje do wysokości równowartości w walucie polskiej 150 euro, ustalonej przy zastosowaniu kursu średniego ogłaszanego przez NBP obowiązującego w dniu wykonania transakcji (art. 46 ust. 2 u.u.p.). Odpowiedzialność ta zostaje jednak rozszerzona do pełnej wysokości, jeżeli płatnik doprowadził do transakcji umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszeniem co najmniej jednego z obowiązków o których mowa w art. 42 u.u.p.

<sup>123</sup> Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, Dz.U. 2011 nr 199 poz. 1175.

<sup>124</sup> Przez usługi płatnicze należy rozumieć w szczególności wykonywanie transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy przez wykonywanie usług polecenia przelewu.

<sup>125</sup> Zob. szerzej: J. Skoczek, *Usługi płatnicze świadczone przez kasy oszczędnościowo-kredytowe. Zagadnienia cywilnoprawne*, Sopot 2013, s. 26.

<sup>126</sup> B. Bajor [w:] *Ustawa o usługach płatniczych. Komentarz*, red. A. Zalcewicz, B. Bajor, Warszawa 2016, s. 201.

Ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy. Jest to wyraz prokonsumenckiego podejścia ustawodawcy, które chroni stronę z natury słabszą w stosunkach z podmiotem profesjonalnym. Podkreślenia wymaga fakt, że zgodnie z art. 45 ust 2 u.u.p. wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja została autoryzowana przez użytkownika. Dostawca jest obowiązany udowodnić okoliczności wskazujące na fakt, że płatnik doprowadził do niej umyślnie lub wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków o których mowa w art. 42 u.u.p, Przykładem rażącego niedbalstwa w kontekście ataku phishingowego może być korzystanie przez płatnika z zainfekowanego komputera, na którym nie został zainstalowany żaden program antywirusowy, albo przechowywanie w łatwo dostępnym miejscu informacji służących do zalogowania się na stronie banku.

### **Zwrot kwot nieautoryzowanych transakcji będących skutkiem phishingu w praktyce sądowej**

We wrześniu 2015 r. Sąd Rejonowy dla Łodzi-Śródmieście w Łodzi wydał wyrok (sygn. akt II C 383/15 ) w sprawie A. T. przeciwko Bankowi (...) Spółce Akcyjnej we W<sup>127</sup>. Powódka korzystała w pozwanym Banku z usług bankowości elektronicznej. W dniu 22 i 23 maja 2014 r. podjęła dziewięć nieudanych prób zalogowania się na stronie, która ukazała się po wpisaniu adresu strony internetowej Banku. Za każdym razem powódka podawała swój login i hasło a także co najmniej dwukrotnie hasło z listy haseł jednorazowych, będących jej narzędziem autoryzacyjnym. Gdy 27 maja 2014 r. udało jej się uzyskać dostęp do konta, okazało się, że z rachunku oszczędnościowego bez jej wiedzy i zgody wykonano przelewy na rzecz nieznanymi beneficjentów w wysokości 19.700 zł. Tego samego dnia A. T. zgłosiła osobiście reklamację w oddziale pozwanego Banku w Łodzi oraz zawiadomiła Policję. Dochodzenie w sprawie podejrzenia popełnienia przestępstwa, polegającego na bezprawnym wpłynięciu na przetwarzanie i przekazywanie danych informatycznych oraz włamaniu po przełamaniu elektronicznych zabezpieczeń rachunku bankowego, z którego następnie dokonano kradzieży pieniędzy umorzono wobec niewykrycia sprawcy przestępstwa. Bank natomiast odmówił zwrotu utraconych środków uznając transakcję płatniczą za autoryzowaną. A. T. wystąpiła przeciwko Bankowi o zapłatę kwoty 19.700zł z odsetkami ustawowymi od dnia 22 maja 2014

---

<sup>127</sup> Wyrok Sądu Rejonowego dla Łodzi-Śródmieście w Łodzi II Wydział Cywilny z dnia 28 września 2015 r., sygn. akt II C 383/15.

r. do dnia zapłaty tytułem odszkodowania za nienależyte wykonanie umowy rachunku bankowego oraz o zasądzenie od pozwanego na jej rzecz zwrotu kosztów procesu.

Sąd Rejonowy dla Łodzi-Śródmieście w Łodzi po rozpatrzeniu sprawy uznał powództwo za uzasadnione co do zasady i w przeważającej mierze także co do wysokości. Zdaniem sądu roszczenie powódki znajduje oparcie w wcześniej przytoczonych przepisach ustawy o usługach płatniczych.

Sąd Rejonowy stwierdził, że Bank wywiązał się z obowiązku zapewnienia poufności instrumentu płatniczego oraz że powódka uchybiła swoim obowiązkom poprzez udostępnienie instrumentu płatniczego nieuprawnionym osobom, aczkolwiek dokonała tego w sposób niezamierzony i nieświadomy. Wskazał ponadto, że co prawda czynności te z punktu widzenia systemu informatycznego Banku były przeprowadzone poprawnie, przy wykorzystaniu właściwych narzędzi autoryzacyjnych, lecz nie można uznać kwestionowanych transakcji płatniczych za autoryzowane, ponieważ powódka nie wyraziła zgody na ich wykonanie. W ocenie sądu nie można jej również przypisać rażącego niedbalstwa w naruszeniu obowiązków o których mowa w art. 42 u.u.p., ponieważ nie udostępniła nikomu celowo listy haseł jednorazowych, korzystała z komputera z legalnym oprogramowaniem oraz zabezpieczonym programem antywirusowym a ujawnienie haseł nastąpiło wskutek ataku phishingowego, którego powódka stała się ofiarą. Mając na uwadze powyższe okoliczności, Sąd zasądził na rzecz powódki kwotę 18.450,81 zł, pomniejszając żądane przez powódkę 19.700 zł zgodnie z dyspozycją art. 46 ust. 2 ( o którym mowa w poprzednim dziale niniejszej pracy). Zasądził ponadto od pozwanego odsetki ustawowe od dnia 5 września<sup>128</sup> do dnia zapłaty oraz zwrot kosztów procesu zgodnie z zasadą stosunkowego ich rozdzielenia.

Kolejny ważny wyrok dotyczący zwrotu kwoty nieautoryzowanych transakcji wydał Sąd Okręgowy w Łodzi w sprawie z powództwa R. M. przeciwko bankowi (...) SA w W. sygn. Akt: I C 1908/14<sup>129</sup>.

Podobnie jak w poprzedniej sprawie powód korzystał w pozwanym Banku z usług bankowości elektronicznej. W dniu 19 listopada 2013 r. po zalogowaniu się na swoje konto zauważył, że ktoś wykonał bez jego zgody i wiedzy szereg przelewów wychodzących na rachunki nieznanych powodowi osób, na łączną kwotę 87.830 zł. Było to możliwe, dzięki sprawnie przeprowadzonemu atakowi phishingowemu. Podczas logowania się do serwisu internetowego Banku poszkodowanemu pojawił się komunikat zachęcający do zainstalowania

<sup>128</sup> Tego dnia Bank wystosował do powódki odpowiedź na reklamację.

<sup>129</sup> Wyrok Sądu Okręgowego w Łodzi I Wydział Cywilny z dnia 27 stycznia 2016 r., sygn. akt: IC 1908/14.

programu o nazwie „M.antywirus”<sup>130</sup>. Chociaż nazwa programu sugeruje, że jest to oprogramowanie antywirusowe, w rzeczywistości służy on przekierowaniu wszystkich wiadomości sms wysłanych do klienta na inny numer. W ten sposób sprawca phishingu uzyskał dostęp do narzędzia autoryzacyjnego poszkodowanego, którym były jednorazowe kody wysyłane drogą sms-ową.

W ciągu paru minut od stwierdzenia wykonania przelewów powód poprzez infolinię złożył pozwanemu reklamację. Nie została ona jednak uznana, bowiem zdaniem banku powód nie zachował należytej staranności. R. M. wniósł więc o zapłatę na swoją rzecz kwoty 88.366 zł wraz z ustawowymi odsetkami liczonymi od 20 grudnia 2013 r. do dnia zapłaty oraz kosztami postępowania, w tym zastępstwa radcowskiego według norm przepisanych.

W ocenie Sądu pozwany bank nie wywiązał się z obowiązków o których mowa w art. 43 ust. 1 u.u.p. tj. nie zapewnił niedostępności indywidualnych zabezpieczeń instrumentu płatniczego dla osób innych niż użytkownik uprawniony do korzystania z niego. Powód natomiast, zdaniem Sądu nie naruszył obowiązków o których mowa w art. 42 u.u.p. w sposób umyślny lub skutek rażącego niedbalstwa, w związku z tym nie odpowiada za nieautoryzowane transakcje płatnicze. Sąd słusznie zauważył, iż powód miał prawo pozostawać w przekonaniu, że komunikat wyświetlający się podczas logowania na stronie Banku faktycznie od niego pochodzi i służy uzyskaniu lepszych zabezpieczeń, zwłaszcza, że komunikat zajmował część strony a w tle wyświetlała się autentyczna witryna Banku. Był też widoczny symbol zamkniętej kłódki oznaczający bezpieczną stronę. Sąd dodał ponadto, że Bank w żaden sposób nie ostrzegał w dacie zdarzenia swoich klientów przed tego typu komunikatami, ani nie informował, że skorzystanie z nich może nieść za sobą negatywne skutki. Podkreślenia zdaniem Sądu wymaga również fakt, że powód niezwłocznie zawiadomił pozwanego o zaistnieniu nieautoryzowanej transakcji płatniczej, tym samym spełnił wymóg o którym mowa w art. 42 ust. 1 pkt 2 u.u.p.

Mając na uwadze powyższe Sąd orzekł, że pozwany zobowiązany jest niezwłocznie zwrócić powodowi kwotę nieautoryzowanych transakcji płatniczych oraz inne dodatkowo pobrane obciążenia jak również koszty zastępstwa procesowego oraz odsetki ustawowe za opóźnienie<sup>131</sup>.

---

<sup>130</sup> Podczas wyświetlania się komunikatu w tle widoczna była rzeczywista strona Banku. Komunikat ten nie wymagał wpisania identyfikatora ani hasła a jedynie numeru telefonu klienta, na który przychodzą kody służące autoryzacji.

<sup>131</sup> Bank pobrał od powoda prowizję za wykonanie przelewu z karty kredytowej w kwocie 536 zł oraz prowizję od przelewów sorbnet w łącznej kwocie 140zł.

## Podsumowanie

Dynamiczny rozwój bankowości internetowej na świecie sprawił, że dokonywanie operacji bankowych stało się niezwykle proste, wygodne i ogólnodostępne. Sprawdzenie stanu konta, wykonanie przelewu, zaciągnięcie kredytu czy też założenie lokaty oszczędnościowej dostępne jest nawet bez wychodzenia z domu. Wspomniane atuty bankowości internetowej wykorzystywane są jednak również do przestępczych celów. Możliwość dotarcia w krótkim czasie do tysięcy potencjalnych ofiar oraz anonimowość, jaką przy wykorzystaniu odpowiedniego oprogramowania daje sieć Internet w połączeniu z wysoką skutecznością przeprowadzanych ataków sprawiły, że zjawisko phishingu przybrało niewyobrażalnie wielką skalę i stanowi realne zagrożenie dla osób korzystających z bankowości elektronicznej.

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych nakłada na bank szereg obowiązków mających zapewnić bezpieczeństwo środków pieniężnych przechowywanych na rachunku bankowym. W przypadku wystąpienia nieautoryzowanych transakcji to właśnie na nim ciąży obowiązek zwrotu utraconej przez płatnika kwoty. Należy jednak pamiętać, że użytkownik uprawniony do korzystania z instrumentu płatniczego również obciążony jest pewnymi obowiązkami, a odpowiedzialność banku uzależniona jest od stopnia ich wypełnienia.

Praktyka sądowa uznająca roszczenia ofiar phishingu o zwrot nieautoryzowanych transakcji stanowi asumpt dla banków do ciągłego ulepszania zabezpieczeń oraz oferowanych narzędzi autoryzacyjnych. Obecnie ciężko znaleźć bank, który nie informowałby na stronie logowania o zasadach bezpieczeństwa oraz potencjalnych zagrożeniach związanych z atakami phishingowymi. Taka praktyka wpływa na podniesienie świadomości użytkowników bankowości internetowej, co z całą pewnością przyczyni się do zmniejszenia liczby ofiar. Trzeba bowiem pamiętać, że ataki phishingowe bazują głównie na ludzkiej niewiedzy i łatwowierności.

### ***O autorze***

Daniel Lubowiecki jest studentem IV roku prawa na Wydziale Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie. Przewodniczący Studenckiego Koła Naukowego Europejskiej Tradycji Prawnej oraz członek Studenckiego Koła Naukowego Praw Człowieka „IUS HOMINI”.

### ***Streszczenie***

Celem niniejszego artykułu jest przedstawienie zjawiska phishingu w ujęciu prawnokryminalistycznym, ze szczególnym uwzględnieniem środowiska bankowości internetowej. Autor w swoich rozważaniach przybliża genezę phishingu, wskazuje metody działania jego sprawców oraz podejmuje próbę prawnokarnej kwalifikacji omawianej problematyki. W artykule poruszono również kwestie odpowiedzialności banku za nieautoryzowane transakcje będące skutkiem ataku phishingowego oraz ukazano praktykę orzekania sądów w tym zakresie.

### ***Summary***

The aim of this article is to present phenomenon of phishing with particular attention to online banking. The Author in his speculations clears out genesis of phishing, methods used by phishing menace and tries to qualify problematic aspects of phishing in reference to law in force. The article also points out responsibility that comes with unauthorized transactions being result of phishing attack and presents practise of adjudicating this offence in court.