Bezpieczeństwo transakcji bankowych w Internecie - poradnik Związku Banków Polskich
Mając na uwadze Państwa bezpieczeństwo, Związek Banków Polskich przedstawia praktyczny poradnik zawierający podstawowe informacje i zasady, o których warto pamiętać. Dzięki nim, Państwa pieniądze będą jeszcze bezpieczniejsze. Przedstawiamy Państwu informacje o wykorzystaniu kart płatniczych oraz dokonywaniu transakcji w sklepach internetowych oraz korzystaniu z dostępu do Państwa pieniędzy za pośrednictwem zdalnych kanałów dostępu - Internetu, telefonu. Warto się z tymi zasadami zapoznać, warto o nich pamiętać.

ZASADY OGÓLNE

1. Pamiętaj, żaden bank nigdy nie wysyła do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację. Banki nigdy nie podają w przesyłanych wiadomościach linków do stron transakcyjnych. Listy, wiadomości e-mail lub telefony w takich sprawach należy traktować jako próbę wyłudzenia poufnych informacji. Nie odpowiadaj na nie przekazując swoje poufne dane. Bezzwłocznie skontaktuj się ze swoim Bankiem i poinformuj o zdarzeniu.

2. Sprawdź na stronie Twojego Banku jakie zabezpieczenia stosowane są w serwisie internetowym. Przy każdym logowaniu bezwzględnie stosuj się do zasad bezpieczeństwa tam opublikowanych. W przypadku pojawienia się jakichkolwiek nieprawidłowości natychmiast skontaktuj się z pracownikiem Banku.

3. Komputer lub telefon komórkowy podłączony do Internetu musi mieć zainstalowany program antywirusowy i musi on być na bieżąco aktualizowany. Niezbędna jest również aktywacja istotnych modułów w pakiecie ochronnym takich jak monitor antywirusowy, skaner poczty czy firewall. Częstym błędem jest wyłączanie wspomnianych modułów w celu redukcji obciążenia systemu.

4. Dokonuj płatności internetowych tylko z wykorzystaniem „pewnych komputerów". Nie dokonuj płatności internetowych z komputerów znajdujących się w miejscach publicznych np. w kawiarenkach internetowych lub na uczelni.

5. Skontaktuj się ze swoim dostawcą Internetu w celu upewnienia się, że korzysta on bezpiecznych kanałów dystrybucji tej usługi. Zwracaj szczególną uwagę na jakość i bezpieczeństwo usług internetowych dostarczanych przez Twojego dostawcę. Jeśli masz jakieś wątpliwości w tym zakresie zawsze masz prawo zapytać się dostawcy o jakość bezpieczeństwa oferowanego przez niego.

6. Instaluj na swoim komputerze tylko legalne oprogramowanie. Programy niewiadomego pochodzenia, w tym ściągane za pośrednictwem programów typu Peer-to-Peer (P2P) mogą być przygotowane przez hakerów i zawierać wirusy lub inne szkodliwe oprogramowanie.

7. Zaleca się okresowe wykonanie skanowania komputera, w szczególności przed wejściem na stronę internetową banku i wykonaniem jakiejkolwiek transakcji. Większość programów antywirusowych przy włączonym monitorze antywirusowym ma detekcję (wykrywalność) taką samą jak skaner antywirusowy i nie ma konieczności skanowania komputera. Jest jednak część programów, których detekcja monitora antywirusowego jest niższa aniżeli skanera, powoduje to jednak lukę w systemie bezpieczeństwa.

8. Aktualizuj system operacyjny i istotne dla jego funkcjonowania aplikacje np. przeglądarki internetowe. Hakerzy stale szukają luk w oprogramowaniu, które są następnie wykorzystywane do przestępstw internetowych. Producenci systemów operacyjnych i aplikacji publikują stosowne „łaty", których celem jest usuwanie podatności ich produktów na ataki przeprowadzane za pośrednictwem znalezionych luk.

9. Nie otwieraj wiadomości i dołączonych do nich załączników nieznanego pochodzenia. Często załączniki takie zawierają wirusy lub inne oprogramowanie, które pozwala na szpiegowanie Twoich działań.

10. Unikaj stron zachęcających do obejrzenia bardzo atrakcyjnych treści lub zawierających atrakcyjne okazje. Szczególnie niebezpieczne mogą być strony internetowe zawierające treści pornograficzne. Ponadto z pozoru niewinne strony zawierające programy typu „freeware" również mogą być bardzo niebezpieczne, ponieważ hakerzy bardzo często dekompilują je uzupełniając o złośliwy kod.

11. Po zalogowaniu do systemu transakcyjnego nie odchodź od komputera, a po zakończeniu pracy wyloguj się i zamknij przeglądarkę.

12. Jeśli przy logowaniu pojawią się nietypowe komunikaty lub prośby o podanie danych osobowych lub dodatkowe pola z pytaniem o hasła do autoryzacji, natychmiast zgłoś problem do swojego Banku.

13. Nie wchodź na stronę internetową Twojego banku za pośrednictwem linków znajdujących się w przychodzących do Ciebie mailach (Phishing). Używaj do tego celu adresu podanego Ci przez Bank, z którym podpisał(aś/eś) umowę o otwarcie i prowadzenia rachunku bankowego. Nie jest również wskazane wykorzystywanie mechanizmu „Zakładek" (Firefox) lub „adresów Ulubionych" (Internet Explorer), gdyż istnieją szkodliwe obiekty, które potrafią modyfikować zachowane tam adresy.

14. Nigdy nie używaj wyszukiwarek internetowych do znalezienia strony logowania Twojego Banku. Wyszukane w nich linki mogą prowadzić do fałszywych stron lub stron zawierających wirusy.

15. Przed zalogowaniem sprawdź, czy połączenie z bankiem jest bezpieczne. Adres witryny internetowej Twojego Banku powinien rozpoczynać się od skrótu: "**https://**", a nie "http://". Brak litery "s" w skrócie "http" oznacza brak szyfrowania, czyli, że Twoje dane są transmitowane przez internet tekstem jawnym, co naraża Cię na ogromne niebezpieczeństwo.

16. Sprawdzaj prawidłowość certyfikatu. Zanim wpiszesz identyfikator bądź login i hasło sprawdź, czy połączenie z bankiem odbywa się z wykorzystaniem szyfrowania. Jeżeli znajdziesz symbol kłódki, kliknij na niego dwa razy, aby sprawdzić, czy wyświetlony certyfikat jest ważny i czy został wydany dla Twojego Banku. Jeśli certyfikat utracił ważność lub nie został wystawiony dla Twojego Banku albo nie można go zweryfikować zrezygnuj z połączenia.

17. Nigdy nie udostępniaj osobom trzecim identyfikatora ani hasła dostępu. Identyfikator jest poufnym numerem nadawanym przez Bank, nie możesz go zmienić.

18. Nie zapisuj nigdzie haseł służących do logowania i pamiętaj o ich regularnej zmianie. Idealnym rozwiązaniem jest zmienianie haseł raz w miesiącu, ale o ile system tego na

Tobie nie wymusi zmieniaj je przynajmniej raz na dwa miesiące używając kombinacji dużych i małych liter oraz cyfr.

19. Sprawdzaj datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.

20. Korzystaj z infolinii udostępnionej przez Twój Bank. Zawsze masz prawo skorzystać z infolinii swojego Banku jeśli masz wątpliwości w zakresie bezpiecznych transakcji bankowych wykonywanych za pośrednictwem internetu.

21. Odwiedzaj regularnie Portal „Bezpieczny Bank" na stronie internetowej ZBP – www.zbp.pl Jeśli chcesz wiedzieć więcej na temat bezpiecznego posługiwania się bankowością elektroniczną, w tym internetową regularnie odwiedzaj ten Portal. Tam fachowcy z zakresu bezpieczeństwa banku wyjaśniają jak uniknąć czyhających w sieci niebezpieczeństw.

22. Zachowaj rozwagę przy przekazywaniu numeru karty. Nie należy udostępniać numeru karty nikomu, kto do nas dzwoni, również w sytuacji, gdy osoba dzwoniąca informuje, że są problemy z komputerem i proszą o weryfikację informacji. Nie ma zwyczaju by firmy dzwoniły prosząc przez telefon o numer karty płatniczej. Jeżeli to my inicjujemy połączenie, również nie należy udostępniać numeru karty przez telefon, gdy nie mamy pewności, że rozmówca zasługuje na zaufanie.

23. Nigdy nie odpowiadaj na pocztę elektroniczną, z której wynika konieczność podania informacji o karcie – zgłoś taką sytuację w swoim Banku. Nigdy też nie odpowiadaj na maile, które zapraszają do odwiedzenia strony internetowej w celu weryfikacji danych, w tym o kartach. Ten rodzaj oszustwa jest nazywany „phishingiem".

24. Nigdy nie podawaj informacji o karcie na stronach, które nie są bezpieczne. Przykładowo strony z treściami pornograficznymi lub strony nieznanych szerzej firm oferujące markowy towar po rewelacyjnych cenach. Przed wprowadzeniu numeru karty w formularzu na stronie należy upewnić się, czy dane przesyłane z formularza są odpowiednio chronione (czyli – upraszczając – czy adres strony z formularzem rozpoczyna się od https i czy strona posiada odpowiednie certyfikaty – te informacje podaje przeglądarka, zazwyczaj w pasku statusu na dole okna).

25. Nie zapisuj kodu PIN na karcie, ani nie przechowuj go razem z kartą. W takich okolicznościach nie tylko działasz niezgodnie z przepisami prawa, ale także w przypadku kradzieży portfela czy portmonetki i posłużenia się Twoją kartą płatniczą bank będzie zwolniony z obowiązku pokrycia powstałej szkody.

26. Chroń swój numer karty i inne poufne kody umożliwiające dokonane transakcji np. numer PIN, numer CVV2 lub CVC2 – ostatnie trzy cyfry numeru umieszczonego na pasku do podpisu na odwrocie karty. Przestępcy mogą wchodzić w ich posiadanie, rejestrując obraz karty np. przy użyciu telefonu komórkowego z aparatem fotograficznym, kamerą video lub w inny sposób.

27. Dokonuj transakcji w znanych i zweryfikowanych przez siebie sklepach internetowych. W przypadku mniejszych serwisów zbadaj ich wiarygodność, na przykład dzwoniąc do takiego serwisu i weryfikując jego ofertę, warunki dokonania transakcji oraz reklamacji. Upewnij się, czy nie jesteś na stronie internetowej podszywającej się pod stronę Twojego banku/sklepu (podobna nazwa i wygląd strony, którą posługują się nieuczciwi naśladowcy w celu zmylenia i wyłudzenia pieniędzy). Zapoznaj się z regulaminem sklepu internetowego, a szczególnie z informacjami dotyczącymi bezpieczeństwa transakcji. Przed dokonaniem transakcji upewnij się, że transmisja odbywa się w bezpiecznym połączeniu za pomocą protokołu SSL/TLS.

Jak banki dbają o bezpieczeństwo swoich klientów:

- Podstawowa identyfikacja klienta: identyfikator + PIN, tonek, token + PIN
- Protokół szyfrowania transmisji danych w Internecie – SSL
- Dostęp w oparciu o certyfikaty
- Kody wysyłane SMS'em
- Jednorazowe kody autoryzujące transakcje
- Podpis elektroniczny, funkcja skrótu i jej zastosowanie
- Karty mikroprocesorowe z zapisanym certyfikatem
- Limity transakcji
- Automatyczne wygasanie sesji po okresie nieaktywności użytkownika

Jakie dane są atrakcyjne dla włamywaczy:

- wszelkie dane osobowe
- hasła
- numery kart płatniczych
- elektroniczne dokumenty zawierające dane bankowe

Bezpieczeństwo komputera w Internecie

1. Co nas chroni

FireWall

Zapora sieciowa (ang. firewall – zapora ogniowa, ściana ognia) – jest jednym ze sposobów zabezpieczania komputerów, sieci i serwerów przed intruzami. Firewall może być zarówno sprzętem komputerowym ze specjalnym oprogramowaniem bądź samym oprogramowaniem blokującym dostęp do naszych zasobów niepowołanym osobom lub programom. Jeszcze kilka lat temu oprogramowanie spełniające rolę firewalla było dostępne i dedykowane właśnie dla ważnych serwerów lub przy dużych sieciach. Jednak wraz z ogromnym tempem wzrostu technologicznego firewall staje się nieodzownym oprogramowaniem każdego domowego komputera podłączonego do sieci lokalnej LAN lub Internetu. Zapora na takim domowym komputerze sprawdza cały ruch sieciowy wchodzący i wychodzący, ogranicza i zabrania dostępu w obydwie strony nieznanym programom lub użytkownikom.

Programy antywirusowe

To oprogramowanie komputerowe, które ma za zadanie wykrywanie, zabezpieczanie, zwalczanie, usuwanie i naprawianie szkód spowodowanych wirusami komputerowymi. Jeśli uruchamiana aplikacja będzie zawierała szkodliwe oprogramowanie wtedy program wykona odpowiedni ruch który wykluczy wirusa i pozwoli na dostęp do uruchamianego programu. Ważną funkcją każdego antywirusa jest odpowiednio częsta aktualizacja definicji wirusów zawartych w programie. Służy do „bycia na bieżąco" w świecie wirusów. Dzięki uaktualnianym definicjom program zbiera informacje o najnowszych wirusach i dostaje instrukcje które pozwalają mu je zwalczać i naprawiać. Szanujące się firmy produkujące programowanie antywirusowe w swoich produktach stosują codzienną aktualizację definicji wirusów.

Programy antyspamowe

To rodzaj oprogramowania służącego do blokowania niechcianej korespondencji przesyłanej drogą elektroniczną. Programy filtrują wiadomości i wykorzystują tak zwane czarne listy adresów i domen używanych przez spamerów. Większość tego typu oprogramowania posiada możliwość ustawiania własnych reguł, które możemy modyfikować i określać np.: słowa-klucze, występujące w materiałach reklamowych blokując tym samym naszą skrzynkę pocztową na wiadomości zawierające te słowa w tytule przesyłki. Jednak programy te nie są bezbłędne i czasem potrafią zablokować korespondencję która powinna być dostarczona

IDS

To system wykrywania włamań (Intrusion Detection System) jego celem jest zidentyfikowanie niebezpiecznych działań zachodzących w sieci. Wyszukuje wszystkie niedozwolone lub podejrzane ruchy w sieci, które mogą stanowić zagrożenie dla systemu. Wykrywa nieudane próby ataku lub przygotowania do pełnego włamania np.: skanowanie portów lub mapowanie sieci poprzez wyszukiwanie jej krytycznych serwerów, usług i aplikacji. Zadaniem sond systemu IDS jest zbieranie informacji, a zadaniem systemu zarządzania obróbka zebranych informacji i wyłowienie z nich sygnałów ataku.

2. Zagrożenia w Internecie

Wirusy

Wirus komputerowy to powielający się segment wykonywalnego kodu umieszczony w innym programie lub sprzężony z nim. Wirus nie może działać sam - potrzebuje nosiciela w postaci programu komputerowego. Po uruchomieniu tego programu zazwyczaj pierwszy uruchamia się złośliwy kod wirusa a następnie właściwy program. Po skutecznej infekcji dalsze działanie zależy od określonego typu wirusa i obejmuje:

- Replikację jedynie w zainfekowanym systemie.
- Infekcję dalszych plików podczas ich uruchamiania lub tworzenia.
- Kasowanie lub uszkadzanie danych w systemach i plikach.
- Marnowanie zasobów systemowych bez powodowania szkód.

Ze względu na rodzaje wirusów można podzielić je na:
- dyskowe – infekują sektory startowe dyskietek i dysków twardych
- plikowe – infekują pliki wykonywalne danego systemu operacyjnego
- wirusy BIOS-owe – niszczą BIOS komputera (oprogramowanie odpowiadające za poprawna konfigurację i start systemu)
- makrowirusy – atakują przez pliki niewykonywalne, np.: pliki dokumentu Word lub Excel, infekcja odbywa się poprzez makra zawarte w tych dokumentach
- wirusy komórkowe - na razie rzadko spotykane, lecz w przyszłości będą stanowić istotne zagrożenie w związku z rozwojem oprogramowania dla telefonów

Robaki

Robak to samoreplikujący się program komputerowy, podobny do wirusa komputerowego. Główną różnicą między wirusem, a robakiem jest to, że podczas gdy wirus potrzebuje nosiciela, który modyfikuje doczepiając do niego swój kod wykonywalny, to robak jest pod tym względem samodzielny i rozprzestrzenia się we wszystkich sieciach podłączonych do zainfekowanego komputera. Oprócz podstawowej funkcji replikacji robak może mieć wbudowane inne funkcje, takie jak niszczenie systemu, wysyłanie poczty i poprzez nią zarażanie następnych komputerów lub instalowanie koni trojańskich. Obecnie robaki wykorzystują wszelkie dostępne sposoby rozprzestrzeniania , jak np.: sieci LAN, Internet, poczta e-mail, sieci wymiany plików, telefony komórkowe. Od kilku lat robaki sieją spustoszenie na całym świecie: przenoszą konie trojańskie, spam, wspomagają przeprowadzanie ataków Dos, powodują awarię systemów i przeciążenia kanałów internetowych.

Spyware

Spyware jest rodzajem złośliwych programów obejmujących aplikację, która bez zgody użytkownika zbiera i wysyła informacje o jego systemie komputerowym. Poza naruszeniem prywatności, programy spyware generują niepotrzebny i obciążający ruch sieciowy, a w przypadku błędów w kodzie mogą spowodować uszkodzenie systemu operacyjnego.

Spoofing
Spoofing – to jedna ze skuteczniejszych i często stosowanych metod nieautoryzowanego pozyskiwania informacji. Polega ona na "podszywaniu" się pod inny komputer w sieci. Haker wysyłając pakiety z fałszywym adresem źródłowym oszukuje komputer-odbiorcę, który błędnie identyfikując nadawcę wszystkie pakiety wysyła bezpośrednio do agresora. W ten sposób komputer hakera może "udawać" np. serwer, dzięki czemu może uzyskać dostęp do wszystkich tajnych danych. Powstało już mnóstwo wersji oprogramowania służącego to tego typu działań. Można je instalować zarówno na komputerze-agresorze jak i samych urządzeniach dostępowych np. routerach. Taki atak na router może być bardzo groźny w skutkach, ze względu na to że cały ruch w nim generowany może być kontrolowany przez hakera. Na szczęście większość markowych routerów posiada zabezpieczenia przed spoofingiem.

Sniffing
Technika ta została stworzona na potrzeby administratorów i polega ona na "podsłuchiwaniu" wszystkich pakietów krążących po sieci komputerowej. Analiza takich pakietów pozwala na łatwe wychwycenie jakichkolwiek nieprawidłowości w funkcjonowaniu sieci. Dzięki monitorowaniu pracy sieci administrator widzi jej słabe i mocne punkty. Sniffing jako narzędzie administracyjne stwarza ogromne możliwości diagnostyczne. Zalety Sniffingu zostały również zauważone przez hakerów. Możliwość przechwycenia wszystkich informacji wymienianych poprzez sieć stanowi dla niech olbrzymią zachętę. Do analizy "śledzonych" pakietów stworzyli oni własne oprogramowanie, które umożliwia wychwycenie ważnych informacji, takich jak hasła, numery kart kredytowych czy dane osobowe. Ograniczeniem zagrożenia związanego ze sniffingiem jest stosowanie bezpiecznego połączenia typu SSL.

Stealware
Stealware (z ang. "Stealing Software" - oprogramowanie okradające) służy do okradania użytkowników z pieniędzy. Moduł okradający śledzi wszelkie poczynania użytkownika w systemie. Gdy ten chce zapłacić za jakąś usługę przez Internet, odpowiedni moduł okradający uaktywnia się i przekierowuje dany przekaz pieniężny na odpowiednie konto. Aktualnie modułów typu Stealware jest niedużo, ale ich liczba szybko wzrasta.

Phishing
To podstępne pozyskanie poufnej informacji osobistej, jak hasła czy szczegóły karty kredytowej, przez udawanie osoby godnej zaufania, której te informacje są pilnie potrzebne. Jest to rodzaj ataku opartego na inżynierii społecznej. Dzisiaj przestępcy sieciowi wykorzystują techniki phishingu w celach zarobkowych. Popularnym celem są banki czy aukcje internetowe. Phisher wysyła zazwyczaj spam do wielkiej liczby potencjalnych ofiar, kierując je na stronę w Sieci, która udaje rzeczywisty bank internetowy, a w rzeczywistości przechwytuje wpisywane tam przez ofiary ataku informacje. Typowym sposobem jest informacja o rzekomym zdezaktywowaniu konta i konieczności ponownego reaktywowania, z podaniem wszelkich poufnych informacji. Częstym sposobem jest również imitacja strony banku internetowego, użytkownik wpisuje wszystkie potrzebne informacje do poprawnego zalogowania się te jednak się nie odbywa, a dane wpisane przez użytkownika uzyskuje phisher.

Konie trojańskie
Koń Trojański jest wirusem komputerowym, choć zasada jego działania znacznie odbiega od działania tradycyjnego wirusa. Koń trojański nie powiela i nie rozprzestrzenia się samodzielnie. Komputer - ofiara infekowana jest tylko poprzez umyślne zainstalowanie przez użytkownika programu-nosiciela. Nosicielem tym może być jakikolwiek program instalowany na komputerze. Podczas instalacji, koń trojański który wkomponowany jest w kod programu, instaluje się w tle a więc nie jest widoczny dla użytkownika. Bardzo często wirusy te rozsyłane są za pomocą poczty elektronicznej w formie

zainfekowanych animacji lub zdjęć, choć najbardziej chyba przewrotnym typem koni trojańskich są programy podające się za narzędzia antywirusowe. Cele ataków konia trojańskiego mogą być różne, głównie jest to przejęcie kontroli nad zainfekowanym komputerem lub zdobycie przechowywanych na nim informacji.

Spam
Spam to niechciana korespondencja rozsyłana drogą elektroniczną w postaci poczty e-mail. Zazwyczaj jest wysyłany masowo. Istotą spamu jest rozesłanie dużej liczby informacji komercyjnych o jednakowej treści do nieznanych sobie osób. Nie ma znaczenia treść tych wiadomości. Spam można porównać do ulotek zostawianych pod drzwiami naszych mieszkań lub dołączanych do naszej korespondencji. W większości przypadków spam służy do celów komercyjnych, w korespondencji elektronicznej namawiają nas na kupno danych artykułów lub wabią wygraną wycieczką. Czasem jednak spam jest narzędziem ataku na nas poprzez próby wydobycia poufnych informacji podszywając się pod bank lub inną instytucję.

Adware
Adware to rodzaj oprogramowania, które w pełnej, funkcjonalnej wersji udostępniane jest za darmo, a którego autor lub producent otrzymuje wynagrodzenie za reklamy zlecane przez sponsorów, wyświetlane najczęściej w oknie programu. Przykładami adware są m.in. Opera, Eudora, GetRight, Gozilla, Gadu - Gadu. Status adware jest zazwyczaj domyślną opcją użytkownik może zrezygnować z uciążliwych bannerów reklamowych wykupując tradycyjną licencję na korzystanie z programu. Programy tego typu zawierają często ukryte funkcje monitorujące poczynania użytkownika mamy wówczas do czynienia ze szpiegowaniem użytkownika i status programu z adware zmienia się na spyware.

Atak hybrydowy
Atak hybrydowy - atak słownikowy z uwzględnieniem możliwych permutacji i zakłócen, np. przekształcanie haseł do gwary crackerskiej, dodawanie do haseł cyfr lub innych znaków nie-alfanumerycznych.

Atak słownikowy
Atak słownikowy to atak polegający na próbie nieautoryzowanego zalogowania się do systemu komputerowego bez znajomości hasła dostępu. W miejsce hasła podstawiane są kolejne słowa znajdujące się w pliku - słowniku. Plik - słownik może zawierać nawet do kilku tysięcy słów. Im jest większy tym większe prawdopodobieństwo trafienia poprawnego hasła. Podstawowa metoda obrony przed atakiem, to częsta zmiana haseł. Ważne jest przy tym, aby używane hasła nie były prostymi słowami znajdującymi się w słowniku np. dom, rower itd. Administrator systemu powinien wymusić na użytkownikach zmianę hasła np. raz na miesiąc. Dobrym pomysłem jest wprowadzenie do haseł dużych i małych liter oraz niestandardowych znaków typu %#@.

Peer-to-Peer (P2P) – jest to model komunikacji w sieci np. internetowej pomiędzy użytkownikami, w którym każdy z użytkowników ma równe prawa. Najczęściej spotykanym modelem P2P są programy służące do wymiany plików w Internecie, gdzie każdy z użytkowników odgrywa rolę serwera – źródła ściąganych plików oraz klienta – użytkownika, który pobiera pliki z innych źródeł-klientów. Wymiana danych w modelu P2P odbywa się zawsze bez pośrednictwa centralnego serwera. Ponadto model P2P jest strukturą odznaczającą się dużą zmiennością, ponieważ zależy od tego, ilu użytkowników w danym momencie jest zalogowanych.

Materiał powstał w Radzie Bankowości Elektronicznej Związku Banków Polskich przy współpracy pracowników banków zajmujących się bezpieczeństwem oraz funkcjonariuszy Policji Państwowej zajmujących się zwalczaniem przestępczości gospodarczej, w tym również przestępstw popełnianych w obszarze bankowości elektronicznej.