Informacja Edukacyjna

Bezpieczeństwo transakcji płatniczych wykonywanych w Internecie i ryzyk związanych z korzystaniem z usług bankowości Internetowej

Mając na uwadze Państwa bezpieczeństwo, Bank Spółdzielczy Rzemiosła w Radomiu zwany dalej Bank 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.

Dbając o bezpieczeństwo systemów bankowości internetowej Bank stosuje:
- protokół szyfrowania transmisji danych w Internecie –SSL;
- Kody wysyłane SMS'em;
- Jednorazowe kody autoryzujące transakcje;
- Karty mikroprocesorowe z zapisanym certyfikatem;
- Limity transakcji;
- Automatyczne wygasanie sesji po okresie nieaktywności użytkownika;
- System bakowości internetowej Banku wymusza zmienię hasła co 60 dni.

Państwo ze swojej strony powinni przede wszystkim chronić:
- dane osobowe;
- loginy;
- hasła;
- numery kart płatniczych;
- elektroniczne dokumenty zawierające dane bankowe oraz instalować i aktualizować programy antywirusowe na swoich urządzeniach.

Aby zachować bezpieczeństwo transakcji płatniczych wykonywanych w Internecie i ograniczyć ryzyko związane z korzystaniem z usług bankowości Internetowej poniżej przedstawiamy Państwu ogólne zasady postępowania o których należy pamiętać i je stosować.

Bezpieczeństwo transakcji bankowych w Internecie

1. **Bank nigdy nie wysyła do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację.**
   Bank nigdy nie podaje w przesyłanych wiadomościach linków do stron transakcyjnych. Listy, wiadomości e-mail lub telefony w takich sprawach należy traktować jako próbę wyłudzenia poufnych informacji. Nie należy odpowiadać na nie przekazując swoje poufne dane. Bezzwłocznie należy skontaktować się z placówką Banku i poinformować o zdarzeniu. Wykaz placówek i numery telefonów znajdują się na stronie internetowej Banku www.bsr.com.pl zwana dalej stroną internetową Banku.
2. **Należy sprawdzić na stronie Banku jakie zabezpieczenia stosowane są w serwisie internetowym.**
   Przy każdym logowaniu bezwzględnie należy stosować się do zasad bezpieczeństwa opublikowanych na stronie internetowej Banku. W przypadku pojawienia się jakichkolwiek nieprawidłowości należy się skontaktować z placówką Banku.
3. **Komputer lub telefon komórkowy podłączony do Internetu musi mieć zainstalowany program antywirusowy i należy go na bieżąco aktualizować.**
   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. **Należy dokonywać 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. **Należy skontaktować się ze swoim dostawcą Internetu w celu upewnienia się, że korzysta on z 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. **Należy instalować 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. **Bank zaleca 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 należy otwierać wiadomości i dołączonych do nich załączników nieznanego pochodzenia.**
   Często załączniki takie zawierają wirusy lub inne oprogramowanie, które pozwala na szpiegowanie Twoich działań.
10. **Należy unikać 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 należy odchodzić od komputera, a po zakończeniu pracy należy się wylogować i zamknąć 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 należy zgłosić problem do Banku.**
13. **Nie należy wchodź na stronę internetową Banku za pośrednictwem linków znajdujących się w przychodzących do Państwa mailach (Phishing).**
    Do tego celu należy używać adresu podanego przez Bank. 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 należy używać wyszukiwarek internetowych do znalezienia strony logowania Banku.**
    Wyszukane w nich linki mogą prowadzić do fałszywych stron lub stron zawierających wirusy.
15. **Przed zalogowaniem należy sprawdzić, czy połączenie z Bankiem jest bezpieczne.**
    Adres witryny internetowej 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 Państwa na ogromne niebezpieczeństwo.
16. **Należy sprawdzać prawidłowość certyfikatu.**
    Zanim wpiszecie Państwo identyfikator bądź login i hasło należy 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 Banku. Jeśli certyfikat utracił ważność lub nie został wystawiony dla Banku albo nie można go zweryfikować należy zrezygnować z połączenia.
17. **Nigdy nie należy udostępniać osobom trzecim identyfikatora ani hasła dostępu.**
    Identyfikator jest poufnym numerem nadawanym przez Bank, nie mogą go Państwo zmienić.
18. **Nie należy zapisywać nigdzie haseł służących do logowania.**
    System bakowości internetowej Banku wymusi zmienię tego hasła co 60 dni, które nie może być identyczne niż 10 wcześniej użytych.
19. **Jeśli mają Państwo wątpliwości w zakresie bezpiecznych transakcji bankowych wykonywanych za pośrednictwem Internetu** należy skontaktować się z Bankiem osobiście lub dzwoniąc do placówki Banku.
20. **Zalecane jest przez Bank regularnie odwiedzanie Portalu „Bezpieczny Bank" na stronie internetowej ZBP – www.zbp.pl**
    Jeśli chcą Państwo wiedzieć więcej na temat bezpiecznego posługiwania się bankowością elektroniczną, w tym internetową zalecamy regularne odwiedzanie Portalu. Tam fachowcy z zakresu bezpieczeństwa banku wyjaśniają jak uniknąć czyhających w sieci niebezpieczeństw.

Bezpieczeństwo płatności kartami płatniczymi przez Internet

1. **Należy zachować 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.
2. **Nigdy nie należy odpowiadać na pocztę elektroniczną, z której wynika konieczność podania informacji o karcie – zgłoś taką sytuację do Banku.**
   Nigdy też nie należy odpowiadać na maile, które zapraszają do odwiedzenia strony internetowej w celu weryfikacji danych, w tym o kartach. Ten rodzaj oszustwa jest nazywany „phishingiem".
3. **Nigdy nie należy podawać 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).
4. **Nie należy zapisywać kodu PIN na karcie, ani nie przechowywać go razem z kartą.**
5. **Należy chronić swój numer karty i inne poufne kody umożliwiające dokonane transakcji np. numer PIN, numer CVV2 – 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 fotograficznych, kamerą video lub w inny sposób.
6. **Należy dokonywać transakcji w znanych i zweryfikowanych przez Państwa sklepach internetowych. W przypadku mniejszych serwisów należy zbadać ich wiarygodność, na przykład dzwoniąc do takiego serwisu i weryfikując jego ofertę, warunki dokonania transakcji oraz reklamacji.**
   Należy upewnić się, czy nie jesteście Państwo na stronie internetowej podszywającej się pod stronę Banku/sklepu (podobna nazwa i wygląd strony, którą posługują się nieuczciwi naśladowcy w celu zmylenia i wyłudzenia pieniędzy). Należy zapoznać się z regulaminem sklepu internetowego, tj. przede wszystkim z informacjami dotyczącymi bezpieczeństwa transakcji. Przed dokonaniem transakcji należy upewnić się, że transmisja odbywa się w bezpiecznym połączeniu za pomocą protokołu SSL/TLS.

Bezpieczeństwo komputera w Internecie co go chroni a co zagraża:

Chroni:
1. **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.

2. **Program antywirusowy** – 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.
3. **Program antyspamowy** – to rodzaj oprogramowania służącego do blokowania niechcianej korespondencji przesyłanej droga 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.
4. **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 ata

Zagraża:

1. **Wirus** – wirus komputerowy to powielający się segment wykonywalnego kodu umieszczony w innym programie lub sprężony 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:
   1) replikację jedynie w zainfekowanym systemie. - Infekcję dalszych plików podczas ich uruchamiania lub tworzenia;
   2) kasowanie lub uszkadzanie danych w systemach i plikach.;
   3) marnowanie zasobów systemowych bez powodowania szkód.

   Wirusy można podzielić na następujące rodzaje:
   1) dyskowe – infekują sektory startowe dyskietek i dysków twardych
   2) plikowe – infekują pliki wykonywalne danego systemu operacyjnego
   3) wirusy BIOS-owe – niszczą BIOS komputera (oprogramowanie odpowiadające za poprawna konfigurację i start systemu)
   4) makrowirusy – atakują przez pliki niewykonywalne, np.: pliki dokumentu Word lub Excel, infekcja odbywa się poprzez makra zawarte w tych dokumentach
   5) wirusy komórkowe - na razie rzadko spotykane, lecz w przyszłości będą stanowić istotne zagrożenie w związku z rozwojem oprogramowania dla telefonów
2. **Robak** – 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.
3. **Spywar** – 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.
4. **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.
5. **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.
6. **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.
7. **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.
8. **Koń trojański** – 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 wiec 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.
9. **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.
10. **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.
11. **Atak hybrydowy** – atak hybrydowy - atak słownikowy z uwzględnieniem możliwych permutacji i zakłóceń, np. przekształcanie haseł do gwary crackerskiej, dodawanie do haseł cyfr lub innych znaków nie-alfanumerycznych.
12. **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 %#@.
13. **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.