

Damian Daszkiewicz

„Wirtualne płatności”

darmowy fragment

Niniejszy **darmowy** ebook zawiera fragment pełnej wersji pod tytułem:

„Wirtualne płatności”

Aby przeczytać informacje o pełnej wersji, [kliknij tutaj](#).

Darmowa publikacja dostarczona przez

www.eksiazki.end.pl

Niniejsza publikacja może być kopiowana, oraz dowolnie rozprowadzana tylko i wyłącznie w formie dostarczonej przez Wydawcę. Zabronione są jakiegokolwiek zmiany w zawartości publikacji bez pisemnej zgody wydawcy. Zabrania się jej odsprzedaży, zgodnie z [regulaminem Wydawnictwa Złote Myśli](#).

© Copyright for Polish edition by ZloteMysli.pl

Data: 27.12.2004

Tytuł: Wirtualne płatności: E-Gold i Moneybookers (fragment utworu)

Autor: Damian Daszkiewicz

Korekta techniczna i skład: Anna Grabka

Niniejsza publikacja może być kopiowana, oraz dowolnie rozprowadzana tylko i wyłącznie w formie dostarczonej przez Wydawcę. Zabronione są jakiegokolwiek zmiany w zawartości publikacji bez pisemnej zgody wydawcy. Zabrania się jej odsprzedaży, zgodnie z [regulaminem Wydawnictwa Złote Myśli](#).

Internetowe Wydawnictwo Złote Myśli

ARCHmedia s.c.

ul. Przy Dolinie 5/9

61-551 Poznań

WWW: www.ZloteMysli.pl

EMAIL: kontakt@zlotemysli.pl

Wszelkie prawa zastrzeżone.

All rights reserved.

SPIS TREŚCI

WSTĘP

WIRTUALNE PŁATNOŚCI

WESTERN UNION

[Gdzie i jak wykonać przelew?](#)

[Cennik \(jeśli płacimy w złotych\)](#)

[Cennik \(jeśli płacimy w dolarach\)](#)

E-GOLD

[Zakładanie konta](#)

[Logowanie](#)

[Sprawdzanie stanu konta i historii](#)

[Jak zrobić przelew?](#)

[Co to jest Turing Number i jakie ma on zastosowanie?](#)

[Przypominanie hasła do konta e-gold](#)

[Program partnerski](#)

[Automatyczne płatności](#)

MONEYBOOKERS

[Zakładanie konta](#)

[Logowanie](#)

[Zasilenie konta](#)

[Przelew środków](#)

[Przypominanie hasła](#)

[Definiowanie konta bankowego](#)

[Wyplata środków na konto bankowe](#)

[Powiadomienia SMS](#)

[Konfiguracja płatności poprzez telefon](#)

[Masowe płatności](#)

[Program partnerski](#)

[Automatyczne płatności](#)

PAYPAL

JAK ZASILAĆ SWOJE WIRTUALNE KONTA BANKOWE?

POPROSZENIE KOGOŚ O ZROBIENIE PRZELEWU

FORUM DYSKUSYJNE

KANTOR.E-GOLD.COM.PL

Tabela prowizji

Jak dokonać wymiany?

PRZELEW BANKOWY

ZASTOSOWANIE WIRTUALNYCH PŁATNOŚCI

AUKCJE INTERNETOWE

Serwisy aukcyjne:

BUBLE GAMES

E-GOLD GAMES

E-GOLD RANDOMIZER

GET PAID TO READ (GPTR)

Polecanie

Chcesz się szybko wzbogacić?

Ciekawy sposób na zarobek w firmach GPTR

Czy warto się reklamować w firmach GPTR?

Inne niebezpieczeństwa

Kto na tym biznesie najwięcej zarabia?

Podsumowanie

HYIPY (OFFSHORE)

PROGRAMY PARTNERSKIE

PRZELEWY

RAPORTY

SPAM NIGERYJSKI

WYSZUKIWARKI

Złośliwe wyszukiwarki

Podsumowanie

ZAKŁADY BUKMACHERSKIE

WIRTUALNE PŁATNOŚCI I BEZPIECZEŃSTWO 6

NIGDY NIE PODAWAJ SWOJEGO HASŁA 6

UWAŻAJ, JAKĄ STRONĘ ODWIEDZASZ 7

ZMIENIAJ HASŁA 7

UŻYWAJ DOBRYCH HASEŁ 7

STOSUJ RÓŻNE HASŁA 8

ZAŁÓŻ DRUGIE KONTO E-GOLD 8

NIGDY NIE KLIKAJ W LINKI W MAILACH 9

UWAŻAJ NA ZAŁĄCZNIKI 10

UŻYWAJ OPROGRAMOWANIA ANTYWIRUSOWEGO 11

NIE WKLEPUJ HASŁA Z KŁAWIATURY 11

PRZECHOWUJ HASŁA W BEZPIECZNYM MIEJSCU 11

AKTUALIZUJ SWOJE OPROGRAMOWANIE 12

KORZYSTAJ Z BEZPIECZNEGO OPROGRAMOWANIA 12

UNIKAJ SPYWARE 13

KONTROLUJ PLIK HOSTS 13

NIGDY NIE BĄDŹ W TYLE 15

DODATEK A: HISTORIA TRANSAKCJI W FORMACIE CSV

DODATEK B: PRZEDRUK ARTYKUŁU „E-ZŁOTO DLA ZUCHWAŁYCH”

ZAKOŃCZENIE

WIRTUALNE PŁATNOŚCI I BEZPIECZEŃSTWO

Wiadomo, że najwięcej oszustów jest tam, gdzie są duże pieniądze. Często słyszymy w telewizji, że ktoś stracił pieniądze, bo robił zakupy w Internecie. Niestety, ale media szukając sensacji, zazwyczaj mówią o negatywnych rzeczach, gdyż są one ciekawsze, niż np. informacje w stylu „Pan Edzio kupił książkę nie wychodząc z domu”. Pogoń za sensacją i ujawnianie informacji o kolejnych wirtualnych kradzieżach powoduje, że ludzie boją się używać wirtualnych kont bankowych. Z jednej strony media mają rację, gdyż takie przypadki się zdarzają, z drugiej strony uważam, że dużo bardziej prawdopodobne jest spotkanie „dresa” który zabierze nam portfel, niż wyczyszczenie np. konta e-gold. Jednak w świecie rzeczywistym można zmniejszyć prawdopodobieństwo spotkania „typa spod ciemnej gwiazdy” stosując się do kilku rad (np. mając dużo gotówki rozdzielić ją na kilka kieszeni, albo nosić drugi portfel, w którym jest 20 zł, nie chodzić w nocy po wąskich uliczkach itp.). Korzystając z wirtualnych płatności, też trzeba przestrzegać minimum zasad bezpieczeństwa, poniżej je opiszę.

Nigdy nie podawaj swojego hasła

To dziwne, ale są osoby, które chętnie podadzą swoje hasło do e-golda. Wystarczy tylko napisać spreparowany e-mail, w którym ktoś się podszyje pod obsługę e-golda i zawsze znajdzie się kilka ofiar, które podadzą hasło. Zapamiętaj raz na zawsze: administrator dowolnego systemu wirtualnych płatności (np. e-gold) nigdy nie zapyta Ciebie o hasło. Administratorzy nie potrzebują haseł! A nawet, jeśli administratorowi byłoby potrzebne Twoje hasło, to z pewnością odczytałby je z bazy danych, co jest szybsze i wygodniejsze niż proszenie o podanie hasła ;-)

Chcę zwrócić na coś Twoją uwagę: nigdy nikomu nie ufaj. To, że w polu **Nadawca** pisze: E-Gold (service@e-gold.com) naprawdę nic nie znaczy. Oszuści coraz częściej pisząc e-mail podszywają się pod kogoś, wpisując adres e-mail tej osoby. Jest to bardzo prosta sztuczka, która niestety powoduje, że już takiej osobie ufamy.

Wyłudzeniem od ludzi haseł zajmują się ludzie, którzy dobrze opanowali socjotechnikę. Więcej o socjotechnice możesz przeczytać w książce wydawnictwa Helion: [Sztuka podstęp. Łamałem ludzi, nie hasła](#), autorstwa samego Kevina Mitnicka (tak naprawdę, on **nie był** świetnym hackerem, on po prostu **po mistrzowsku wyłudzał hasła**).

Uważaj, jaką stronę odwiedzasz

Oszuści często korzystają z nieuwagi użytkowników. Np. aby zalogować się na swoje konto e-gold, należy wejść na stronę internetową www.e-gold.com. Musisz jednak bardzo ostrożnie wpisać adres tej strony, gdyż istnieją strony o podobnych adresach, wyglądające jak oryginalna, a ich celem jest wydobycie hasła od użytkownika. Np. często ludzie popełniają literówki i zamiast www.e-gold.com wpisują www.e-godl.com. Również istnieje strona www.e-qold.com (litery **q** i **g** są bardzo podobne). Zawsze adres strony internetowej wpisuj powoli i sprawdź, czy nie popełniłeś prostej literówki zanim się zalogujesz! Jeśli się zalogujesz, to administrator fałszywej strony będzie znał Twoje hasło!

Zmieniaj hasła

Zachęcam do częstego zmieniania hasła do e-golda (nie rzadziej niż co 3 miesiące). Często osoba, która pozna hasło na e-golda nie kradnie pieniędzy od razu, tylko obserwuje konto, czekając, aż pojawi się na nim większa suma (np. otrzymasz wypłatę od jakiejś firmy GPTR). Dlatego zachęcam do częstego zmieniania hasła. W dobrym tonie jest zmiana hasła, korzystając z bezpiecznego komputera tuż po tym, jak zaczniesz podejrzewać, że złapałeś jakiegoś wirusa. Polecam też zmianę hasła tuż po otrzymaniu dużej sumy na konto.

Używaj dobrych haseł

Dobre hasło, to takie, które trudno odgadnąć. Jeśli Twoim hasłem jest imię ulubionego aktora, albo data urodzenia, to z dużym prawdopodobieństwem ktoś, kto Ciebie zna może odgadnąć hasło. Warto stosować hasło, które trudno odgadnąć i nie jest słowem w języku

polskim. Dobre hasło powinno składać się zarówno z liter (dobrze by było, gdyby w hasła były używane duże i małe litery) jak i cyfr.

Dlaczego nie warto jest używać hasła, które są wyrazami w danym języku? Otóż crackerzy posiadają słowniki zawierające wszystkie wyrazy w danym języku i w pierwszej kolejności używają programów, które pobierają po kolei wyrazy ze słownika i próbują je wpisać jako hasło.

Stosuj różne hasła

Często użytkownicy Internetu wszędzie używają tylko jednego hasła. Bez wątpienia, jest to wygodne, gdyż nie trzeba pamiętać kilkunastu haseł. Z drugiej strony, jest to bardzo niebezpieczne. Jeśli poznam Twoje hasło to będę mógł dużo narozrabiać. Często nawet zapisując się do firmy wysyłającej płatne e-maile podajemy to samo hasło, jakiego używamy do swojego konta e-gold. Jest to bardzo nieodpowiedzialne, gdyż nie masz gwarancji, że administrator takiej firmy mailowej nie sprawdza, czy przypadkiem nie używasz do e-golda takiego samego hasła. Dlatego przynajmniej do e-golda używaj innego hasła niż do pozostałych rzeczy!

Załóż drugie konto e-gold

Często osoby, które coś sprzedają przez Internet (np. usługi projektowania stron WWW) posiadają dwa konta e-gold: pierwsze do otrzymywania wpłat, a drugie zapasowe. Konto zapasowe służy do przechowywania większej ilości pieniędzy. Nawet, jeśli ktoś się włamie na pierwsze konto, to na drugim koncie zostanie część gotówki. Często osoby, które dużo zarabiają (np. projektują strony WWW) i podają numer swojego konta na stronie, są narażone na atak, gdyż złodziej wie dobrze, że na tym koncie prawdopodobnie jest dużo pieniędzy.

Uwaga

Zgodnie z regulaminem e-golda, nie można posiadać dwóch kont, ale ten zapis można bardzo łatwo obejść, zakładając konto na innego członka rodziny.

Nigdy nie klikaj w linki w mailach

Często oszuści wysyłają wiadomość, że należy zaktualizować swoje dane. Link niby prowadzi na stronę e-golda (lub banku internetowego np. mBank), a tak naprawdę ładuje się strona na serwerze oszusta, której celem jest przechwycenie Twojego hasła. Poniżej przedstawiam e-mail, jaki dostał mój znajomy:

Do:
Temat: [mBank] Aktualizacja danych
Data: Tue, 14 Sep 2004 10:19:58 +0200
Od: mBank <mailing-return@mbank.com.pl>
Adres zwrotny: noreply@mbank.com.pl

Szanowni Klienci,

w trosce o bezpieczeństwo kont naszych Klientów mBank przeprowadza regularne aktualizacje swoich baz danych. Aby zagwarantować bezpieczeństwo Państwa konta prosimy o potwierdzenie chęci dalszego użytkowania z naszych usług przez Internet. W tym celu prosimy wszystkich użytkowników o zweryfikowanie swoich danych dostępowych pod adresem:

<http://www.mbank.com.pl/aktualizacja/>

z góry dziękujemy za Państwa współpracę.

Zespół mBanku

Wiadomość wygląda bardzo wiarygodnie. Nawet, o dziwo, link jest do strony mBanku. Ale to tylko pozory, po najechaniu kursorem myszy na link, pojawia się prawdziwy adres strony:

Do:
Temat: [mBank] Aktualizacja danych
Data: Tue, 14 Sep 2004 10:19:58 +0200
Od: mBank <mailing-return@mbank.com.pl>
Adres zwrotny: noreply@mbank.com.pl

Szanowni Klienci,

w trosce o bezpieczeństwo kont naszych Klientów mBank przeprowadza regularne aktualizacje swoich baz danych. Aby zagwarantować bezpieczeństwo Państwa konta prosimy o potwierdzenie chęci dalszego użytkowania z naszych usług przez Internet. W tym celu prosimy wszystkich użytkowników o zweryfikowanie swoich danych dostępowych pod adresem:

<http://www.mbank.com.pl/aktualizacja/>

z góry dziękujemy za Państwa współudział. Adres: http://www.m-bank.biz/

Zespół mBanku

Wpisz tutaj szybką odpowiedź do: noreply@mbank.com.pl

Tak naprawdę, jest to jedna z prostszych sztuczek, często oszuści potrafią lepiej zamaskować fałszywy adres. Dlatego nigdy nie klikaj w linki w e-mailach, zawsze ręcznie wklepuj dany adres! Poza tym, zwróć uwagę na zamieszczone zrzuty ekranu, pole **Do:** jest puste, co już wyraźnie sugeruje, że coś jest nie tak. Zazwyczaj w polu **Do:** pojawia się Twój adres e-mail, jeśli go nie ma, to z dużym prawdopodobieństwem można wywnioskować, że bank nie jest nadawcą wiadomości.

Naprawdę należy uważać, gdyż ostatnio oszuści podszywają się pod kilka różnych banków internetowych, a także pod e-golda!

Uważaj na załączniki

Często wirtualni złodzieje wysyłają e-mail z jakimś ciekawym programem (teledyskiem, wygaszaczem ekranu, tapetą itp.). Zazwyczaj taki załącznik spełnia dwie role: pierwsza to rola użyteczna np. wygaszacz ekranu pokazuje jakieś ładne widoki, a druga to funkcja szpiegowska, taki wygaszacz to, tak naprawdę program szpiegowski, który może wysłać autorowi informacje o naciskanych klawiszach, (więc jeśli taki program jest

uruchomiony, a Ty w danej chwili logujesz się na swoje konto, to autor owego wygaszacza ekranu będzie znał Twoje hasło). Dlatego lepiej nigdy nic nie uruchamiaj, dopóki nie masz pewności, że dany program wysłał Tobie Twój znajomy (wirusy często podszywają się pod kogoś, kto ma Ciebie w książce adresowej, abyś myślał, że ta osoba wysłała Tobie wiadomość). Bardzo często takie programiki szpiegujące mogą być w komputerze przez kilka miesięcy, dlatego dla własnego bezpieczeństwa nie uruchamiaj załączników.

Używaj oprogramowania antywirusowego

Wirusy też mogą wysyłać autorowi różne informacje (np. mogą na dysku szukać plików, gdzie są zapisane numery wyglądające jak numer karty kredytowej). Dlatego **OBOWIĄZKOWO** musisz mieć zainstalowany jakiś program antywirusowy, który cały czas monitoruje system! Musisz również minimum **RAZ W TYGODNIU** aktualizować definicje wirusów, gdyż codziennie powstaje kilka nowych wirusów, a program bez aktualnych definicji wirusów nie będzie Ciebie bronił przed najnowszymi!

Nie wklepuj hasła z klawiatury

Nawet jeśli będziesz się stosował do podstawowych zasad bezpieczeństwa, nie masz absolutnej pewności, że nie złapiesz jakiegoś wirusa (trojana), który będzie Ciebie szpiegował. Dlatego jeśli jest możliwość, to logując się np. na swoje konto e-gold, hasło wpisuj z wirtualnej klawiatury, gdyż wirusy bardzo często wysyłają autorowi informacje o naciskanych klawiszach.

Przechowuj hasła w bezpiecznym miejscu

Nigdy nie zapisuj haseł do różnych serwisów w pliku tekstowym na pulpicie, (gdyż wirusy mogą poszukiwać takich plików). Najlepiej w ogóle nie trzymaj haseł w komputerze (a jak już, to używaj jakiegoś programu, który jest do tego przeznaczony, gdyż takie programy KODUJĄ wprowadzone hasła), ani w postaci elektronicznej. Nie masz jednak

gwarancji, że autor takiego programu sam nie otrzymuje wklepywanych haseł, dlatego do zapisywania haseł polecam zwykły notesik, który będziesz trzymał w bezpiecznym miejscu.

Telefony komórkowe nie nadają się jako notatnik do przechowywania haseł, gdyż sam bez większego problemu potrafię ze swojego telefonu odczytać notatki, które są chronione przed dostępem kodem PIN2 (więcej informacji na ten temat znajdziesz na stronie: <http://www.daszkiewicz.net/tk-11-2004.php>)

Aktualizuj swoje oprogramowanie

Ponieważ najpopularniejszy system operacyjny Windows, a także przeglądarka stron internetowych Microsoft Internet Explorer i program pocztowy Outlook Express to programy, które nie są pozbawione wad, należy często szukać łatek. W nowszych wersjach systemu operacyjnego Windows jest moduł Windows Update, który aktualizuje system. Zachęcam do aktualizacji przynajmniej raz w miesiącu, gdyż można bezpłatnie usunąć różne błędy, które te programy posiadają. Zazwyczaj kilka dni po wykryciu danej luki pojawiają się wirusy, które ją wykorzystują. Należy zawsze mieć aktualne łatki, gdyż tylko to zmniejsza prawdopodobieństwo złapania wirusa.

Korzystaj z bezpiecznego oprogramowania

Programy Microsoftu posiadają dużo luk bezpieczeństwa. Z jednej strony programiści Microsoftu nie przykładają dużej wagi do bezpieczeństwa, a z drugiej najwięcej osób używa oprogramowania tej firmy, więc jest większe prawdopodobieństwo, że ktoś wykryje jakąś lukę. Ponieważ obawiam się różnych wirusów, używam przeglądarkę internetową Opera a do odbierania poczty służy mi M2 (program mailowy wbudowany w Operę). Dość duża grupa wirusów atakuje tylko Internet Explorera (i Outlook Express), gdyż te programy są najpopularniejsze, natomiast używając mniej popularnych programów, jesteś mniej narażony na różne wirusy. Często mój kolega używający IE łapie różne świństwa, które zmieniają stronę startową. Ja używam Opery i nigdy nie złapałem takiego czegoś!

Przeglądarki internetowe:

Opera - <http://www.opera.com/> (posiada program pocztowy)

Mozilla - <http://mozillapl.org/> (posiada program pocztowy)

FireFox - <http://www.firefox.pl/>

Programy do odbierania poczty:

The Bat - <http://www.ritlabs.com/en/products/thebat/>

Pegasus Mail - <http://www.pmail.com/>

Unikaj spyware

Ta porada ma dużo wspólnego z używaniem bezpiecznego oprogramowania. W skrócie mógłbym powiedzieć: nie instaluj nic poza samym systemem operacyjnym. Spyware to różnego rodzaju programiki szpiegujące, zawarte w innych programach. Niektóre programy są darmowe, ale w zamian za to są wyświetlane reklamy i tutaj się pojawia problem, gdyż niektóre programy oprócz wyświetlania reklam mogą Ciebie szpiegować, albo nawet umożliwiają komuś obcemu zdalne grzebanie na Twoich dyskach (w celu wykradania haseł). Dlatego nigdy nie instaluj zbędnych programów, szczególnie tych, które mają licencje Adware.

W Internecie można również znaleźć programy, które usuwają różne programiki szpiegujące, albo nawet znane programy okrojone z funkcji szpiegujących (np. Kaaza Lite).

Do usuwania programów szpiegujących (spyware) polecam program Ad-Aware, który można ściągnąć z tej strony:

<http://www.pcworld.pl/ftp/pc/katalog/105/ochrona.prywatnosci.html>

Kontroluj plik hosts

Plik hosts zawiera bazę DNSów, z której Windows korzysta. Adres każdej strony to tak naprawdę numer IP, przeglądarka internetowa po wpisaniu adresu strony WWW sprawdza, jaki numer IP jej odpowiada i ładuje tą stronę. Jeśli chcesz poczytać newsy w serwisie onet.pl to możesz wpisać adres <http://www.onet.pl>, albo [http:// 213.180.130.200](http://213.180.130.200).

W pliku hosts można wpisać numery IP i odpowiadające im nazwy serwerów, tak aby przeglądarka internetowa nie musiała się łączyć z serwerem DNS w celu sprawdzenia jaki numer IP odpowiada danemu serwerowi, co pozwala na szybsze załadowanie strony WWW. Oszuści mogą zmodyfikować ten plik tak, że zamiast strony e-golda będzie łądowna się spreparowana strona oszustów (może mieć taki sam wygląd jak strona e-golda!) i, co najważniejsze, nie będziesz o tym wiedział, że zostałeś przekierowany na fałszywą stronę, gdyż przeglądarka internetowa będzie pokazywała adres wpisanej przez Ciebie strony, a tak naprawdę łądowna się strona oszusta!! Aby temu zapobiec, należy sprawdzać plik hosts (plik ten znajduje się w katalogu **Windows**, (jeśli masz Windows 9x lub ME) lub **windows\system32\drivers\etc** (jeśli masz Windows XP) i u mnie ma nazwę **hosts**). Plik ten można otworzyć w notatniku. Domyślnie plik wygląda tak:

```
# Copyright (c) 1998 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP stack for Windows98
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97  rhino.acme.com      # source server
# 38.25.63.10  x.acme.com           # x client host

127.0.0.1    localhost
```

Linie zaczynające się od znaku # to komentarze, których system operacyjny nie bierze pod uwagę. Jeśli znajdziesz wpisy inne niż:

```
127.0.0.1    localhost
```

a nie wiesz, co one oznaczają, to lepiej je usunąć.

Uwaga

Do nadzorowania plików hosts możesz użyć darmowego programu ze strony:

<http://www.pnet.pl/~jelcyn/freesoft/win/HostsFilesChecker.htm>

Porada

W ramach ćwiczenia, które pozwoli lepiej zrozumieć opisywane zagadnienie możesz do pliku hosts dopisać następujące linijki:

213.180.130.200 wp.pl

213.180.130.200 www.wp.pl

Po wyedytowaniu pliku hosts należy ponownie uruchomić komputer a później należy załadować w przeglądarce internetowej stronę wp.pl (lub www.wp.pl).

To ćwiczenie pozwoli nie tylko zrozumieć opisywany problem, ale równie dobrze możesz komuś zrobić dowcip ;-).

Nigdy nie bądź w tyle

Niestety, ale zaraz po wykryciu pewnej luki, albo opracowaniu przebiegłego sposobu wyłudzenia haseł, ludzie są o tym informowani i stają się bardziej czujni, a im bardziej dana luka zostanie nagłośniona, tym więcej osób ściągnie różne „łatki” (im więcej osób przeczyta informacje o jakimś sposobie wyłudzenia haseł, tym trudniej będzie kogoś oszukać, stosując „starą” technikę). Z tego też powodu ludzie szukają nowych luk (lub nowych sposobów wyłudzenia haseł). Aby nie być w tyle, warto być trochę nieufnym. A jeśli interesuje Cię temat bezpieczeństwa, mogę Tobie polecić ciekawego darmowego ebooka: <http://bezpieczny-e-gold.prv.pl/>

Jak skorzystać z wiedzy zawartej w pełnej wersji ebooka?

Powyższy ebook to zaledwie fragment publikacji, która dotyczy wirtualnych płatności w Internecie, transferów pieniężnych zza granicy i bezpieczeństwa takich transakcji. Jeśli myślisz poważnie o zarabianiu, czy handlowaniu w Internecie i chcesz to robić skutecznie i bezpiecznie, zajrzyj na stronę:

<http://egold-moneybookers.zlotemysli.pl/>

