

## Zagrożenia w Internecie

Adres szkolnej  witryny konkursu

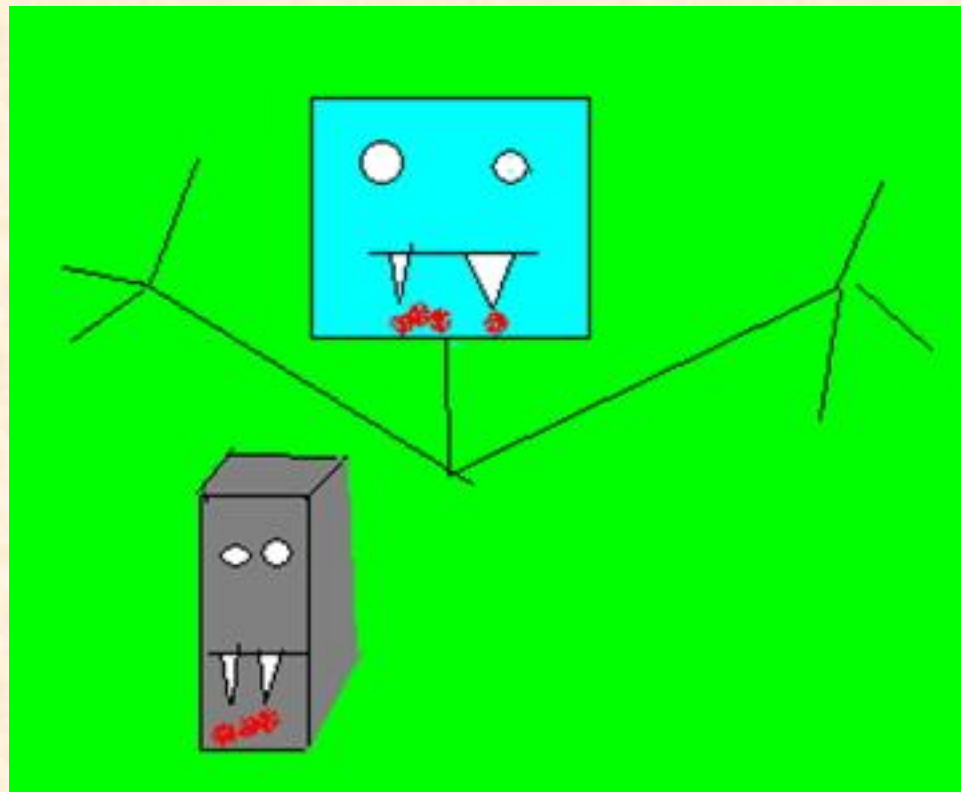
<http://www.tp.webserwer.pl/kbi/>

Szczecin 2011



## Rodzaje złośliwego oprogramowania

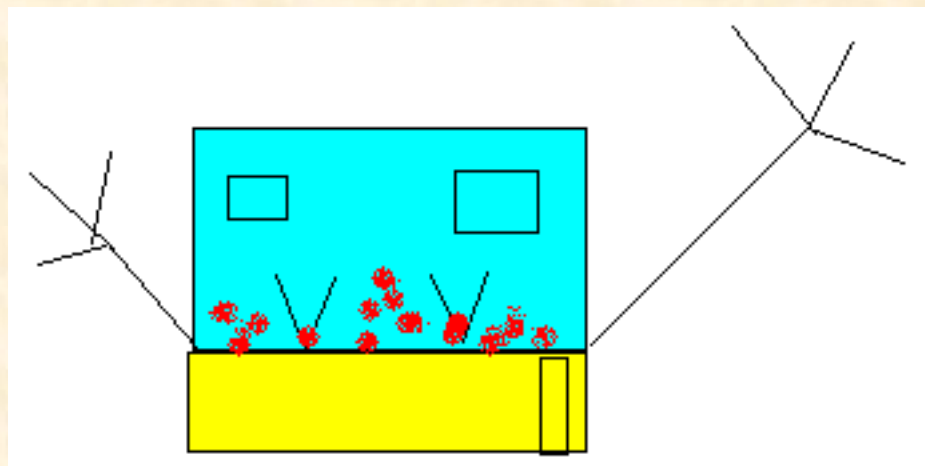
- Malware
- Spyware
- Trojan
- Rootkit
- Spam
- Phishing
- Wirusy i robaki





# Malware

Ogólna nazwa wszystkich aplikacji i skryptów o szkodliwym działaniu wobec użytkownika komputera.



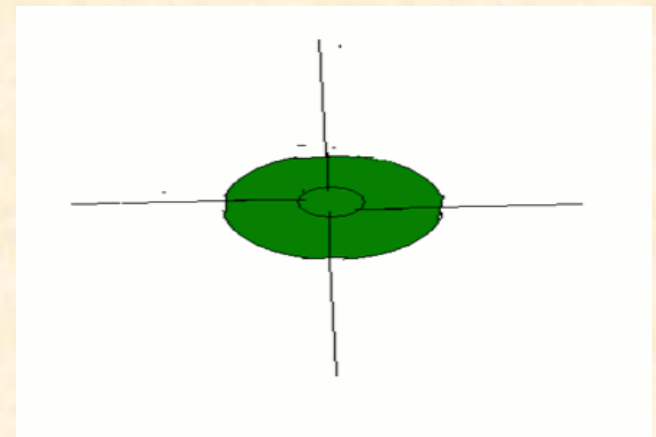


# Programy szpiegujące (ang. *spyware*) – do szpiegowania działań użytkownika

Programy te gromadzą informacje o użytkowniku i wysyłają je często bez jego wiedzy i zgody autorowi programu.

Do takich informacji należeć mogą:

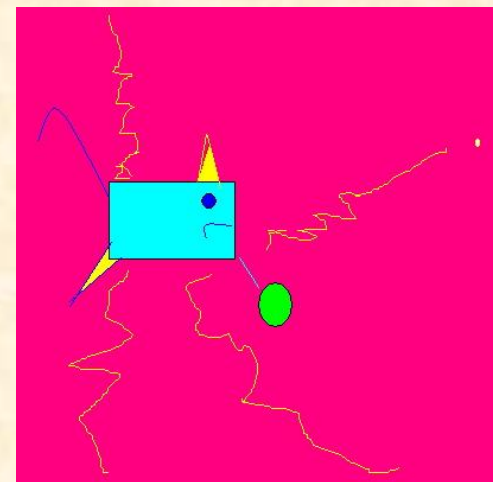
- adresy stron WWW odwiedzanych przez użytkownika,
- dane osobowe,
- numery kart płatniczych,
- hasła,
- zainteresowania użytkownika,
- adresy poczty elektronicznej,
- archiwa.





## Trojan

**Koń trojański** to określenie oprogramowania, które daje hakerowi możliwość kontrolowania komputera bez wiedzy jego użytkownika.





# Rootkit

Program, który w systemie ukrywa obecność swojego i innego oprogramowania hackerskiego. Zazwyczaj blokuje oprogramowanie antywirusowe. Ukrywa on niebezpieczne pliki i procesy, które umożliwiają utrzymanie kontroli nad systemem. Może on np. ukryć siebie oraz konia trojańskiego przed administratorem oraz oprogramowaniem antywirusowym. Rootkit może się dostać do komputera użytkownika wraz z aplikacją będącą w rzeczywistości trojanem.



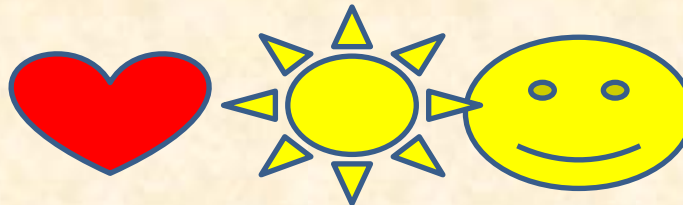




# Spam

Niechciane lub niepotrzebne wiadomości elektroniczne. Najbardziej rozpowszechniony jest spam za pośrednictwem poczty elektronicznej. Część użytkowników doświadcza także spamu w komunikatorach (np. ICQ czy Gadu-Gadu). Istotą spamu jest rozsyłanie dużej ilości informacji o jednakowej treści do nieznanym sobie osób. Nie ma znaczenia, jaka jest treść tych wiadomości.

WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM  
WITAM

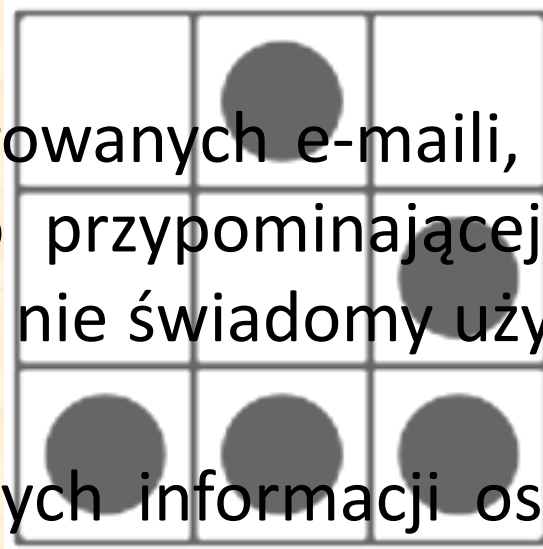


# Phishing

Atak socjotechniczny oparty na inżynierii społecznej.

Polega na:

- wysyłaniu spreparowanych e-maili, które kierują ofiarę do witryny łudząco przypominającej np. stronę banku ofiary, gdzie niczego nie świadomy użytkownik wpisuje na niej login i hasło,
- wyłudzeniu poufnych informacji osobistych (np. haseł lub szczegółów karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne.








Oprogramowanie rozpowszechniające swoje kopie.  
Wirusy infekują pliki wykonywalne, robaki rozpowszechniają się za pomocą poczty i komunikatorów.

- słabość zabezpieczeń systemów komputerowych,
- luki w systemie operacyjnym,
- niedoświadczenie użytkowników,
- naiwność i beztroskę użytkowników.



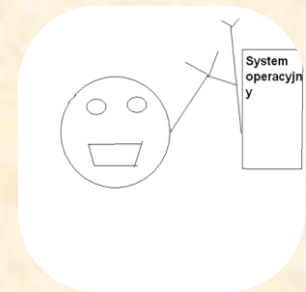
Do zwalczania, usuwania i zabezpieczania się przed wirusami używane są programy antywirusowe.





# Co zwiększa ryzyko w Internecie?

- Oczywiste, łatwe do odgadnięcia hasła dostępu.
- Brak aktualizacji systemu i aplikacji.
- Ujawnianie informacji osobistych online.
- Nadmiar zaufania.
- Nieaktualna ochrona antywirusowa.
- Brak dodatkowych zabezpieczeń.
- Ignorancja i liczenie na cud „mnie to się nigdy nie przytrafi”.





## Włamania hakerów

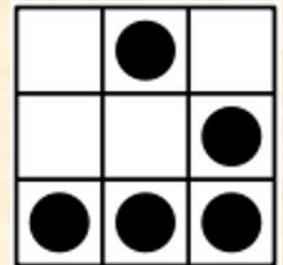
**do komputerów - popularną formą ataków.**

Do włamań hakerzy wykorzystują:

- słabe zabezpieczenia,
- luki w systemach operacyjnych nazywane exploitami.

Haker po wejściu do systemu:

- szuka luk w innych programach,
- uzyskuje prawa administratora systemu,
- instaluje trojana, umożliwiającego przejęcie kontroli nad systemem w innym czasie.

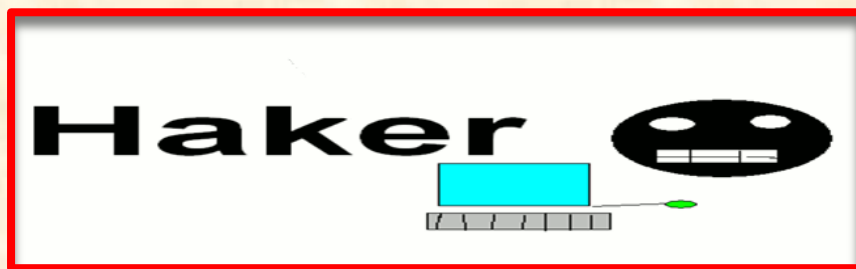


Równie częstymi atakami są ataki typu Dos i DDoS.



# Komputery zombie

**Komputery zombie** – maszyny, nad którymi dzięki trojanom kontrolę przejęli hakerzy. Najczęściej służą do ataków typu DoS (Denial of Service), w których na dany adres wysyłana jest w jednej chwili gigantyczna liczba zapytań, by go zablokować. Ich inne zastosowanie to rozsyłanie spamu.





# Fałszywe strony WWW

Hakerzy tworzą fałszywe strony internetowe np. banku, sklepu i wyłudniają informacje od logujących się użytkowników.

- Jeśli sklep internetowy ma stronę WWW w domenie drugiego lub trzeciego poziomu (np. firma.a.b.pl) lepiej zrezygnować z zakupów. Szanująca się firma zawsze znajdzie pieniądze na zarejestrowanie domeny pierwszego rzędu (np. firma.pl).
- Sprawdź, gdzie i kiedy została zarejestrowana domena wykorzystywana przez sklep internetowy, gdzie jest zlokalizowana obsługa sklepu oraz czy podany adres i numer telefonu są prawdziwe.

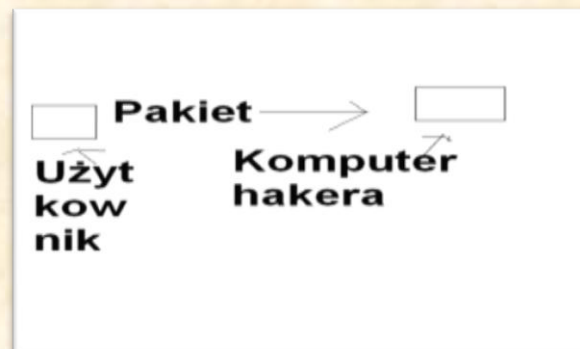
[www.sklep.ax.bx.pl](http://www.sklep.ax.bx.pl)



# Sniffer pakietów

**Sniffer** - program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i ewentualne analizowanie danych przepływających w sieci.

Sniffer stanowi narzędzie diagnostyczne dla administratorów sieci. Może być również stosowany do monitorowania aktywności sieciowej osób trzecich, co jest w większości przypadków niezgodne z prawem.

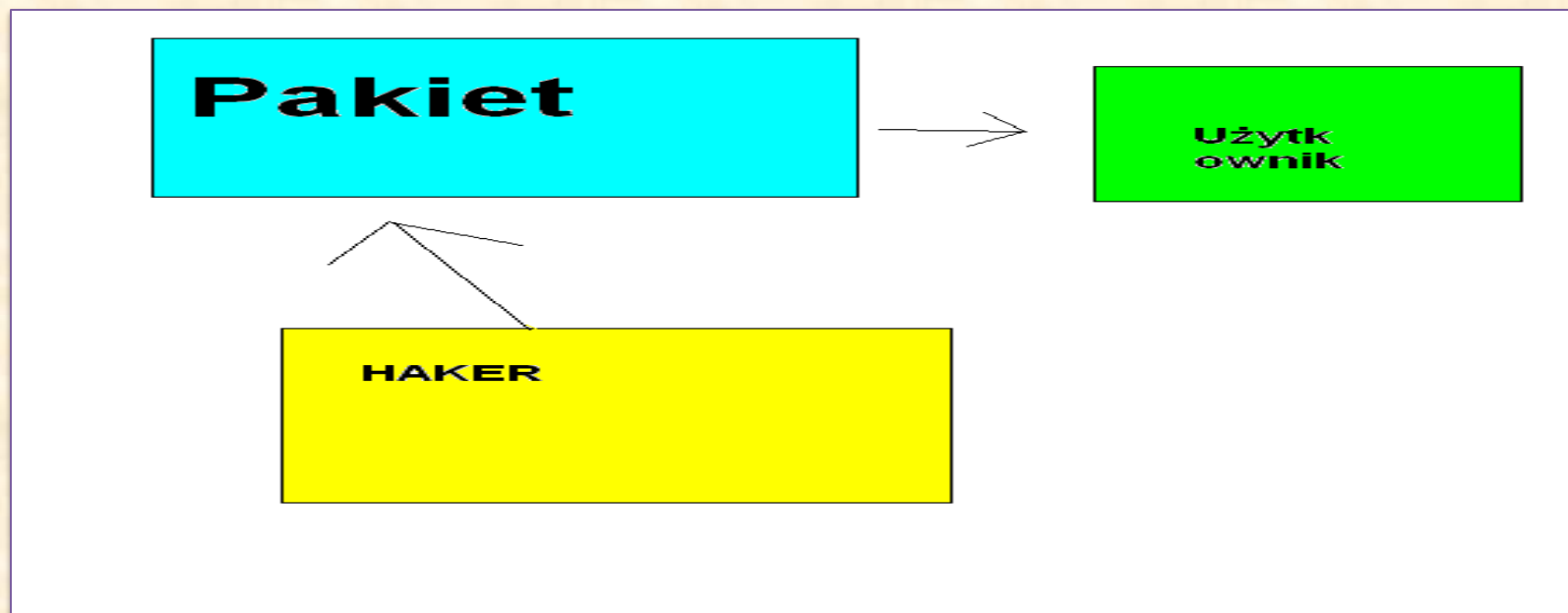






## Spoofing

Spoofing - jest to proces fałszowania pakietów wykonanych w celu podania się za inny komputer, np. serwer WWW, usług pocztowych lub DNS.





# Riskware

**Riskware** – oprogramowanie, które nie jest złośliwe, lecz ze względu na swoje możliwości przy nieumiejętnym stosowaniu może być niebezpieczne dla użytkownika.

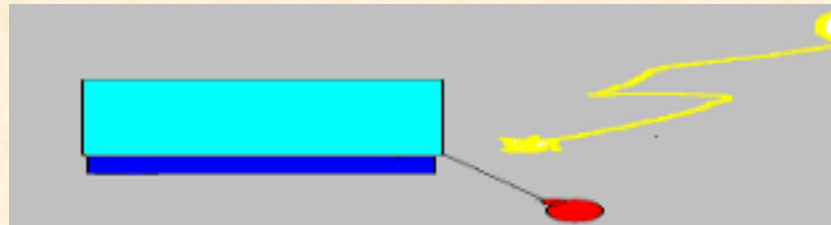
Przykładem jest rodzina programów VNC i NX – służących do zdalnej pracy na komputerze. Gdy użytkownik ustawi w tym programie łatwe do odgadnięcia hasło lub zostawi je „puste”, wówczas atakujący haker może bardzo łatwo przejąć kontrolę nad takim komputerem.



# Keyloggery

**Keylogger** - typ programów komputerowych służących do wykradania haseł.

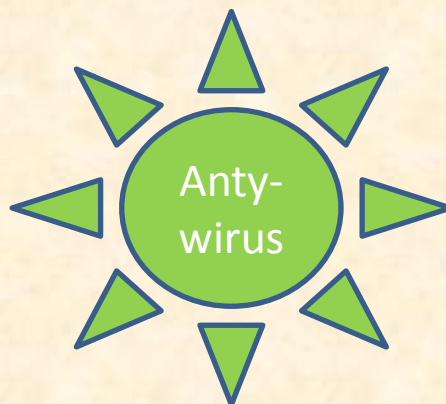
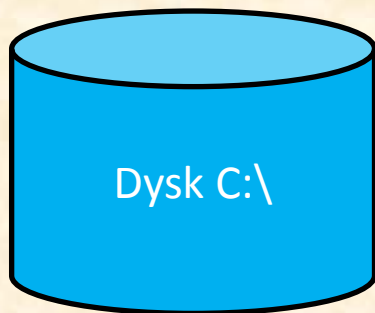
Keyloggery zawierają funkcje chroniące je przed wykryciem przez niedoświadczonego użytkownika komputera, a plik w którym zapisywane są dane ukryty jest np. w katalogach systemowych. Większość keyloggerów ma specjalnie stworzoną funkcję, która pozwala na wysłanie pliku z hasłami na wyznaczony adres pocztowy.





# Obrona przed zagrożeniami

Hakerzy nieustannie rozwijają swoje metody, aby poznać nasze nawyki i sposoby korzystania z komputera. Nowe techniki atakowania pozwalają im być ciągle o krok przed oprogramowaniem zabezpieczającym i przechytrzać nawet przecznych i znających się na zabezpieczeniach użytkowników.

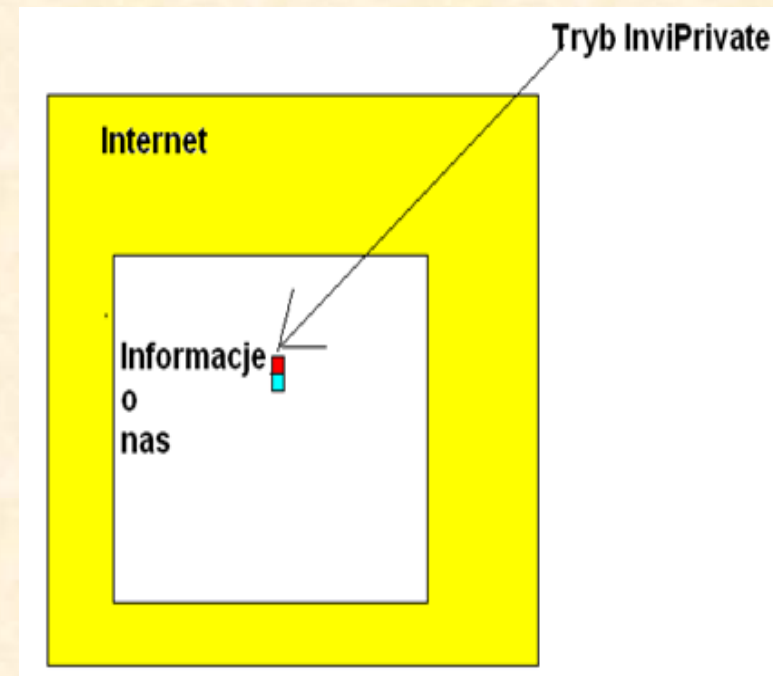


Haker



# Tryb InPrivate

Tryb przeglądania InPrivate pozwala przeglądać sieć Web bez pozostawiania śladów w programie Internet Explorer. Dzięki temu inni użytkownicy komputera nie dowiedzą się o odwiedzanych miejscach i informacjach wyszukiwanych w sieci Web.





# Zabezpieczanie danych

- Szyfrowanie danych za pomocą programu szyfrującego.
- Stosowanie silnych haseł:
  - ✓ przynajmniej 8 znaków,
  - ✓ duże i małe litery, liczby, znaki specjalne.
- Ustawienie hasła do BIOS-u, dysku twardego.
- Wykorzystanie funkcji odzyskiwania danych.

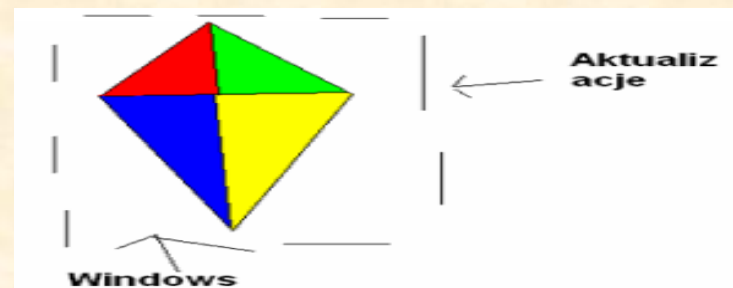
**Md2fg%St76@bc**





# Aktualizacje

Aktualizacje systemu operacyjnego i zainstalowanych aplikacji blokują wtargnięcia różnych szkodników do komputera. Choć produkty Microsoftu stanowią największy cel, luki i niedociągnięcia zdarzają się także w Linuksie i Mac OS X. W miarę jak te systemy operacyjne zdobywają coraz większą popularność stają się jednocześnie coraz bardziej atrakcyjnymi celami dla cyberprzestępców. Ci zaś coraz częściej atakują, wykorzystując luki w programach niezależnie od typu systemu operacyjnego.





# Ujawnianie informacji osobistych online

Portale społecznościowe:

•Facebook: [pl.facebook.com/](http://pl.facebook.com/)

•Nasza – klasa: [nasza-klasa.pl](http://nasza-klasa.pl)

Ujawnianie zbyt wielu informacji o swoim życiu na niezabezpieczonych stronach społecznościowych umożliwia hackerowi przeprowadzenie skutecznego spersonalizowanego ataku. Przejęcia kontroli nad kontem i jego zablokowania agresorzy mogą dokonać, stosując phishing, złośliwe oprogramowanie i inne metody. Przywłaszczonego w ten sposób konta mogą nadużywać do wysyłanie niechcianej korespondencji, podkradania osobistych informacji, a nawet do naciągania na duże pieniądze znajomych właściciela profilu.



## Literatura

- Chip. Styczeń 2007. Hakerzy w natarciu.
- Chip 02 / 2007. Koniec mitu.
- PC Format 4 / 2010. Poznaj swojego wroga.
- Wikipedia. – wolna encyklopedia (<http://pl.wikipedia.org/>)
- Witryna konkursu „Bezpieczny Internet”:
- <http://www.tp.webserwer.pl/kbi/>



# Koniec

