

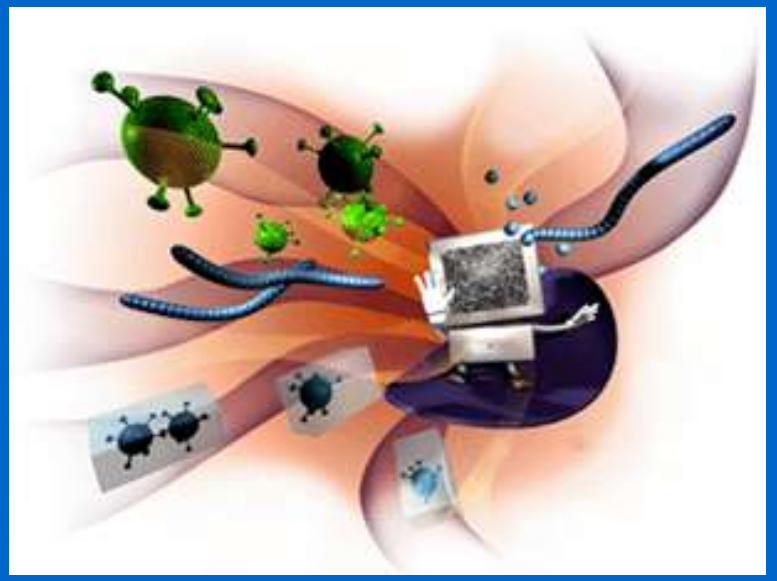

# Internet / Tworzenie stron WWW

## Bezpieczeństwo

Wojciech Sobieski

Olsztyn 2005

# Zagrożenia Internetowe



**Podstawowe zagrożenia:**

- spam
- wirusy komputerowe
- blokowanie serwerów
- podmiana stron WWW
- kradzież danych (hasła, numery kart płatniczych, dane osobowe)
- wyłączenie komputera
- kasowanie i niszczenie danych
- wyświetlanie napisów lub rysunków na ekranie
- uniemożliwienie pracy na komputerze
- przejęcie kontroli nad komputerem
- niszczenie sprzętu komputerowego

# Zagrożenia Internetowe

**Spam** - to elektroniczne wiadomości masowo rozsyłane do osób, które ich nie oczekują. Najbardziej rozpowszechniony jest spam za pośrednictwem poczty elektronicznej.

Istotą spamu jest rozsyłanie dużej liczby wiadomości o jednakowej treści do nieznanych sobie osób. Nie ma znaczenia jaka jest treść tych wiadomości. Rozsyłanie znacznej liczby maili w dowolnej "słusznej sprawie" również jest uważane za spam.

Spam dzieli się na ***U**nsolicited **C**ommercial **E**mail* (UCE), czyli spam komercyjny o charakterze reklamowym, oraz ***U**nsolicited **B**ulk **E**mail* (UBE), czyli niechciane maile o charaktarze niekomercyjnym takie jak "łańcuszki szczęścia", masowe rozsyłanie ostrzeżeń o wirusach, czy masowe rozsyłanie próśb o pomoc.

# Zagrożenia Internetowe

**Wirus komputerowy** – to najczęściej prosty program komputerowy, który w sposób celowy powiela się bez zgody użytkownika. Wirusy wykorzystują słabość zabezpieczeń systemów komputerowych lub właściwości systemów oraz niedoświadczenie i beztroskę użytkowników.

# Zagrożenia Internetowe

**Koń trojański** – program, który nadużywa zaufania użytkownika wykonując bez jego wiedzy dodatkowe, szkodliwe czynności. Konie trojańskie często podszywają się pod pożyteczne programy jak np. zapory sieciowe czy wygaszacze ekranu. Koń trojański jest trudno wykrywalny i może być poważnym zagrożeniem dla bezpieczeństwa systemu.

# Zagrożenia Internetowe

**Bomba logiczna** - rodzaj wirusa, który może pozostać w ukryciu przez długi czas. Jego aktywacja następuje w momencie nadejścia określonej daty lub wykonania przez użytkownika określonej czynności.

# Zagrożenia Internetowe

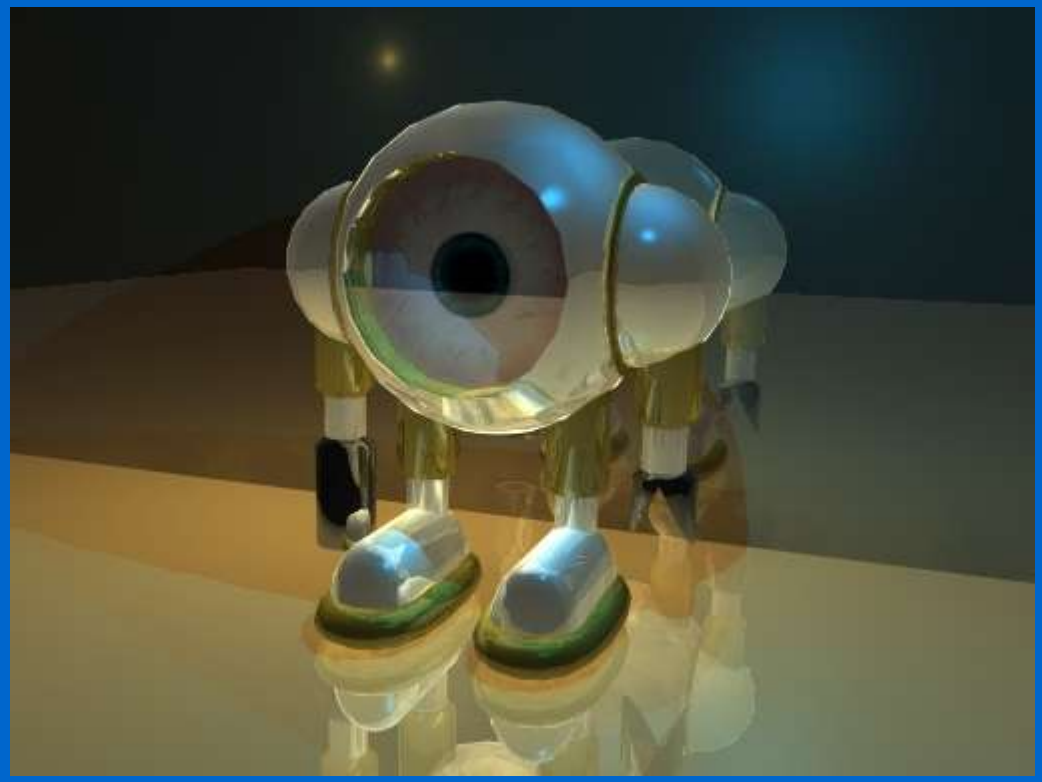
**Robak** - mały, ale bardzo szkodliwy wirus. Do prawidłowego funkcjonowania nie potrzebuje nosiciela. Rozmnaża się samoistnie i w sposób ciągły, powodując w bardzo krótkim czasie wyczerpanie zasobów systemu. Wirusy tego typu są zdolne w bardzo krótkim czasie sparaliżować nawet dość rozległą sieć komputerową.

# Zagrożenia Internetowe

**Dialer** - jest to prosty program łączący korzystającego z modemu użytkownika Internetu ze stronami WWW poprzez wysoko płatne numery dostępowe (0-700). Jest on niewielki (15-90kb), aby jego ściągnięcie było niemal niezauważalne dla użytkownika. Programy tego typu uruchamiają się zazwyczaj wraz ze startem systemu i są zaprojektowane w sposób maksymalnie utrudniający ich usunięcie z komputera. Najczęściej instalują kilka swoich kopii i dokonują zmian w ustawieniach dial-up (odpowiadają one za sposób łączenia się z siecią) tak aby łączenie z internetem odbywało się poprzez numer specjalny należący do producenta dialera, a nie ten wybrany przez użytkownika.

# Zagrożenia Internetowe

**Bot -** jest programem wykonującym pewne czynności w zastępstwie człowieka. Czasem jego funkcją jest udawanie ludzkiego zachowania lub wykonywanie zautomatyzowanych czynności. Jest to w zasadzie prosta sztuczna inteligencja.



# Zagrożenia Internetowe

**Sniffer** (ang. wąchacz) – jest to program komputerowy, którego zadaniem jest przechwytywanie i ewentualne analizowanie danych przepływających w sieci.

Sniffer stanowi nieodzowne narzędzie diagnostyczne większości administratorów sieci, zwłaszcza podczas diagnostyki problemów z niezawodnością lub wydajnością połączeń. Może być również stosowany do monitorowania aktywności sieciowej osób trzecich, co jest w większości przypadków niezgodne z prawem. W celu ochrony przed takimi atakami, niektóre protokoły komunikacyjne stosują mechanizmy kryptograficzne

# Zagrożenia Internetowe

**Phishing** – w branży komputerowej, oszukańcze 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.

# Zagrożenia Internetowe

Nie odpowiadamy na żadne maile zawierające prośby o podanie danych lub o zalogowanie się na jakiejś stronie

Nie klikamy na żadne linki do stron WWW zawarte w przesyłanej do nas poczcie elektronicznej

Nie uruchamiamy żadnych załączników załączonych do poczty elektronicznej

Nie uruchamiamy żadnych programów ściągniętych ze stron WWW lub z nieznanego źródła

Używamy programów antywirusowych, firewalli i zwalczających spyware, malware

Uaktualniamy często system i oprogramowanie za pomocą odpowiednich łatek i uaktualnień ściąganych tylko ze strony producenta

Nie przesyłamy mailem żadnych danych osobistych typu hasła, numery kart kredytowych itp.

W połączeniach z naszym bankiem internetowym wpisujemy jego adres WWW ręcznie korzystając tylko z protokołu https a nie http

Sprawdzamy otrzymane wyciągi papierowe z historią naszych transakcji

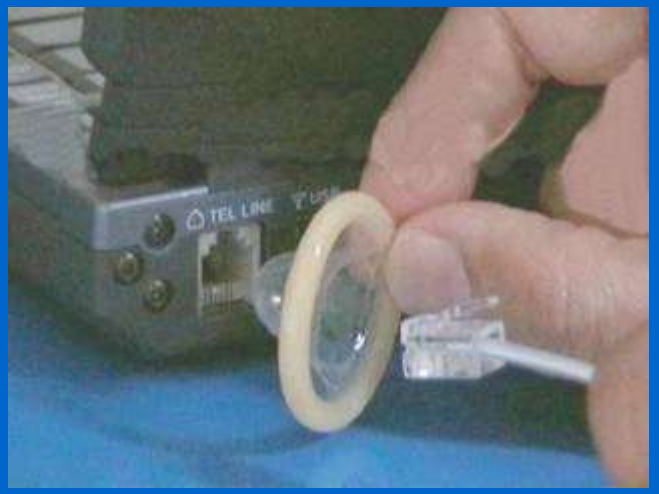
Nie używamy przeglądarek internetowych, które bywają często podatne na różne błędy ale korzystamy z uważanych za bardziej bezpieczne takie jak Mozilla czy Opera

# Zagrożenia Internetowe


**Podstawowe zagrożenia wśród dzieci:**

- kontakt z treściami pornograficznymi
- kontakt z przemocą
- kontakt z pedofilami
- uzależnienie od Internetu
- kontakt z internetowymi oszustami
- nieświadome uczestniczenie w działaniach niezgodnych z prawem
- konsekwencje finansowe (np. korzystanie z dialerów, aukcje)
- nieświadome udostępnianie informacji
  (np. numerów kart, adresów, haseł)

# Ochrona komputera



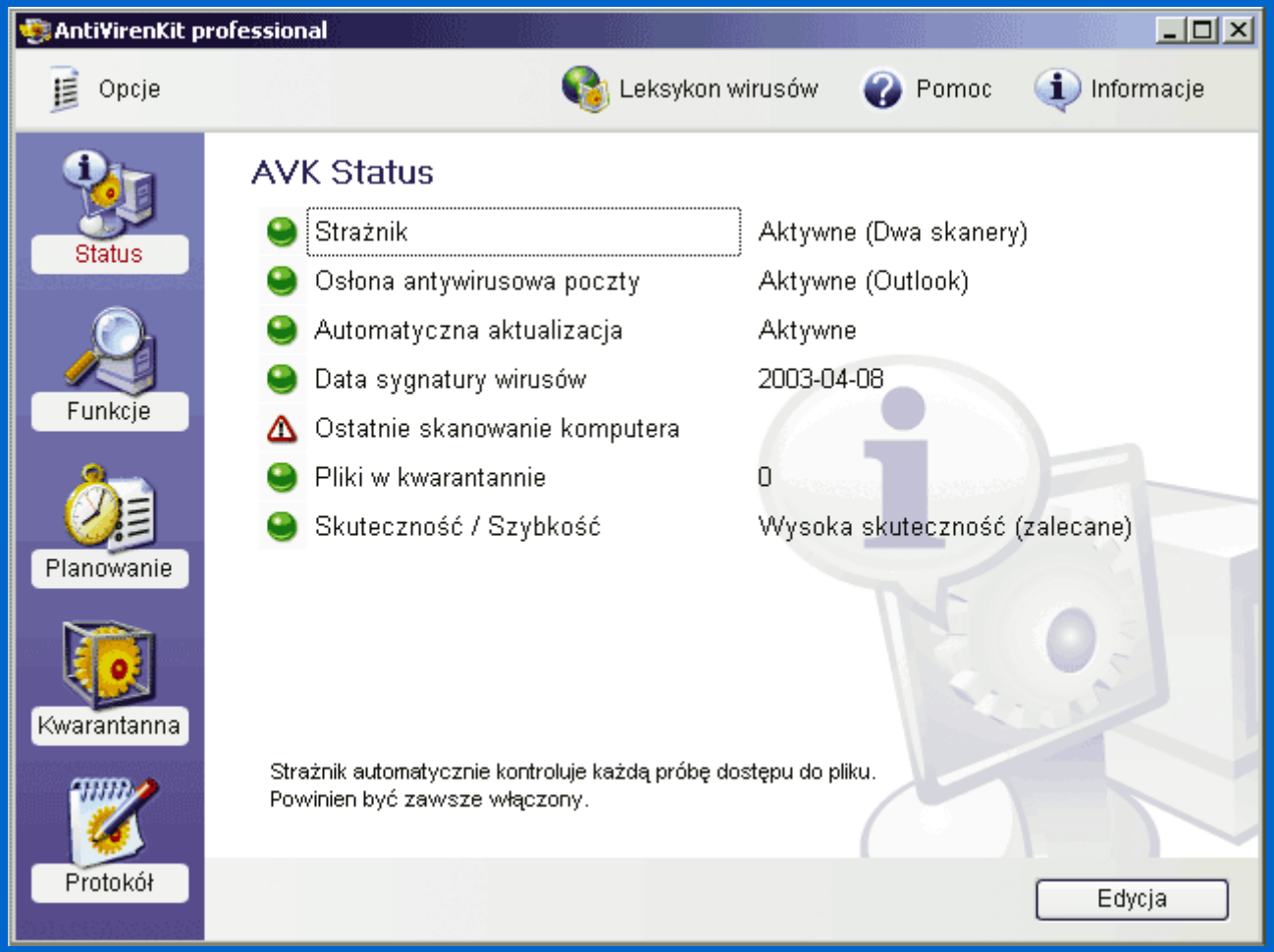
**Podstawowe zasady ochrony:**

- ***antywirusy***
- ***antyspamery***
- ***antydialery***
- ***firewalle***
- skanery rejestru systemowego
- oprogramowanie chroniące system i rejestr systemowy
- czyszczenie plików tymczasowych i plików ***cookies***
- stosowanie i częsta zmiana haseł
- rezygnacja z instalacji nieznanego oprogramowania
- odpowiedni wybór systemu operacyjnego
- zabezpieczanie i ***backup*** danych
- obrazy dysków i partycji
- dbałość o system i jego regularna konserwacja

# Ochrona komputera


***Programy antywirusowe***
***AntiVir Personal: http://www.free-av.com/index.htm***

# Ochrona komputera

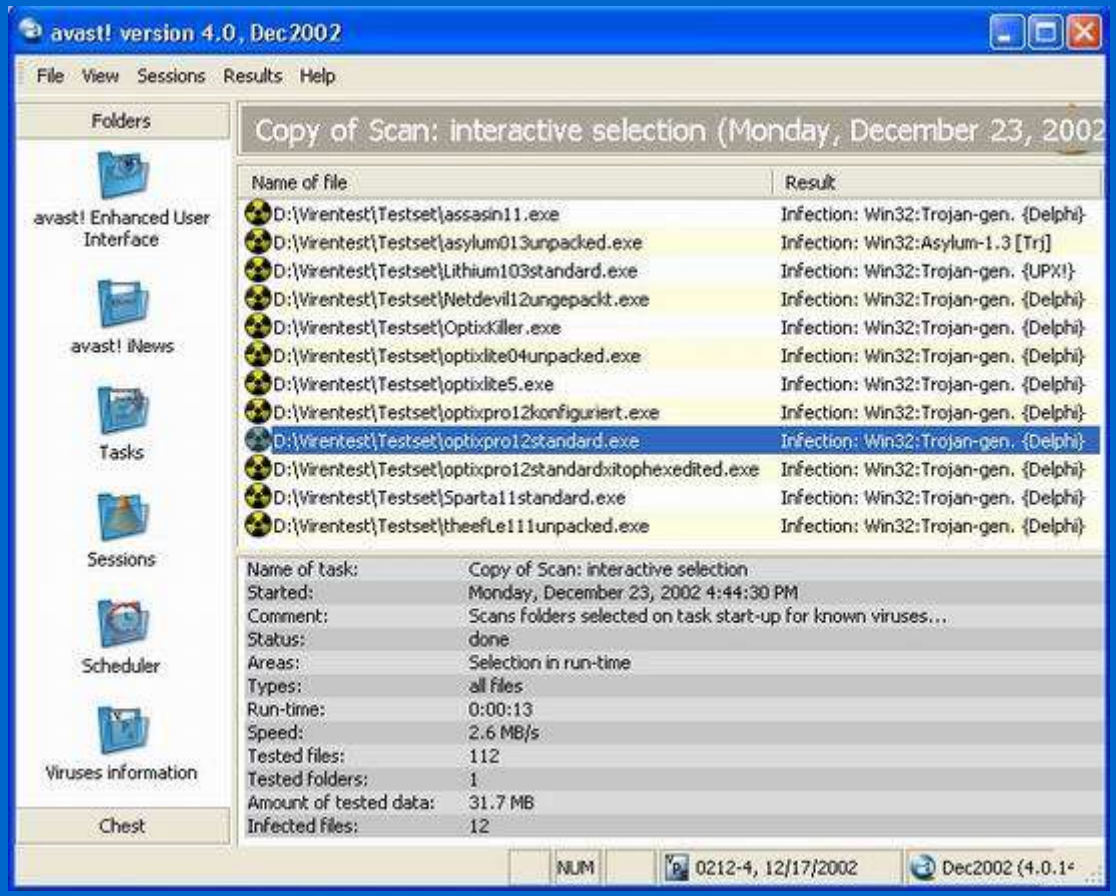



***Programy antywirusowe***
***AntiVirenKit: http://www.gdata.pl/***

# Ochrona komputera

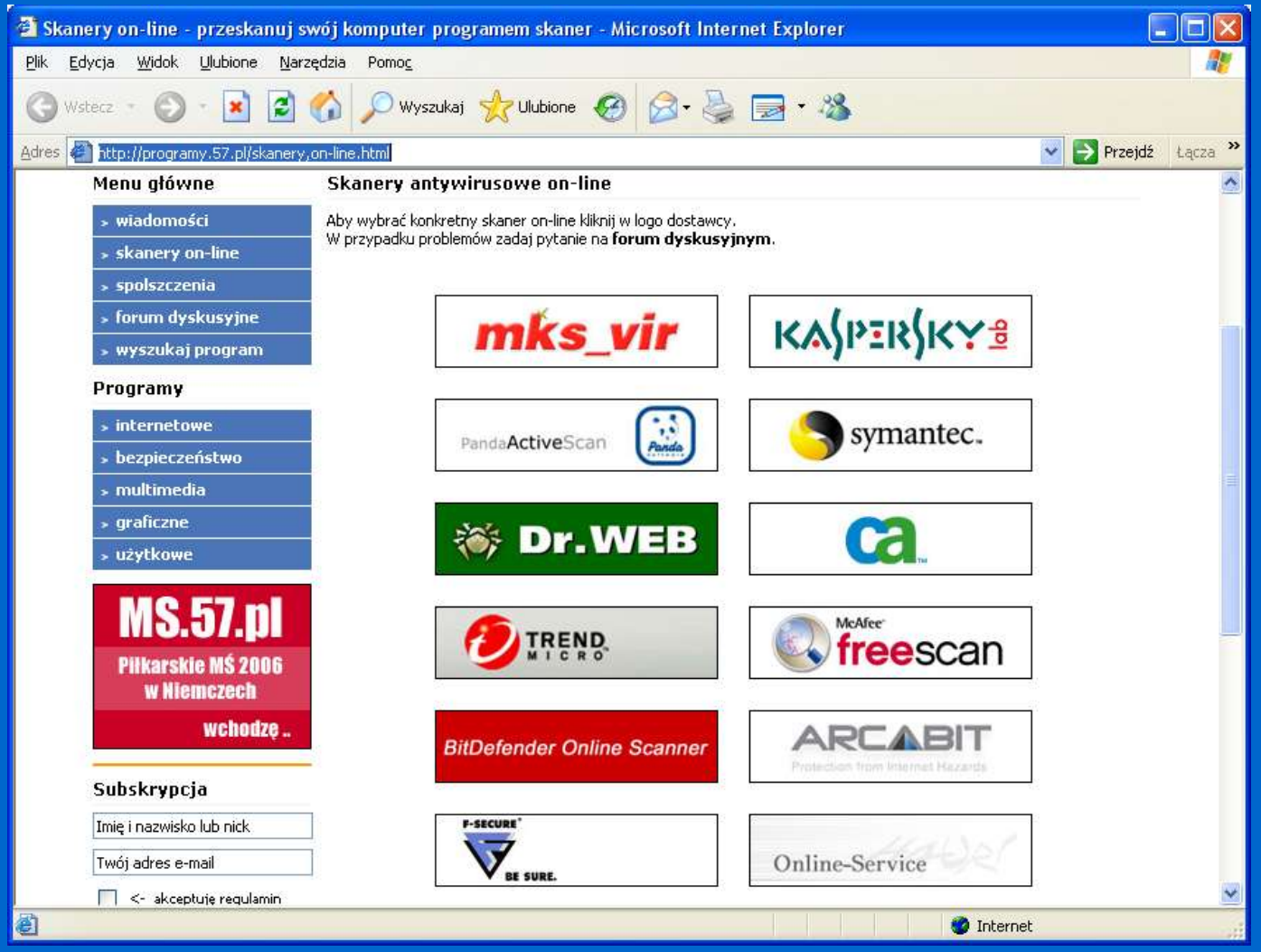

***Programy antywirusowe***
***Kaspersky Anti-Virus: http://www.kav.pl/***

# Ochrona komputera



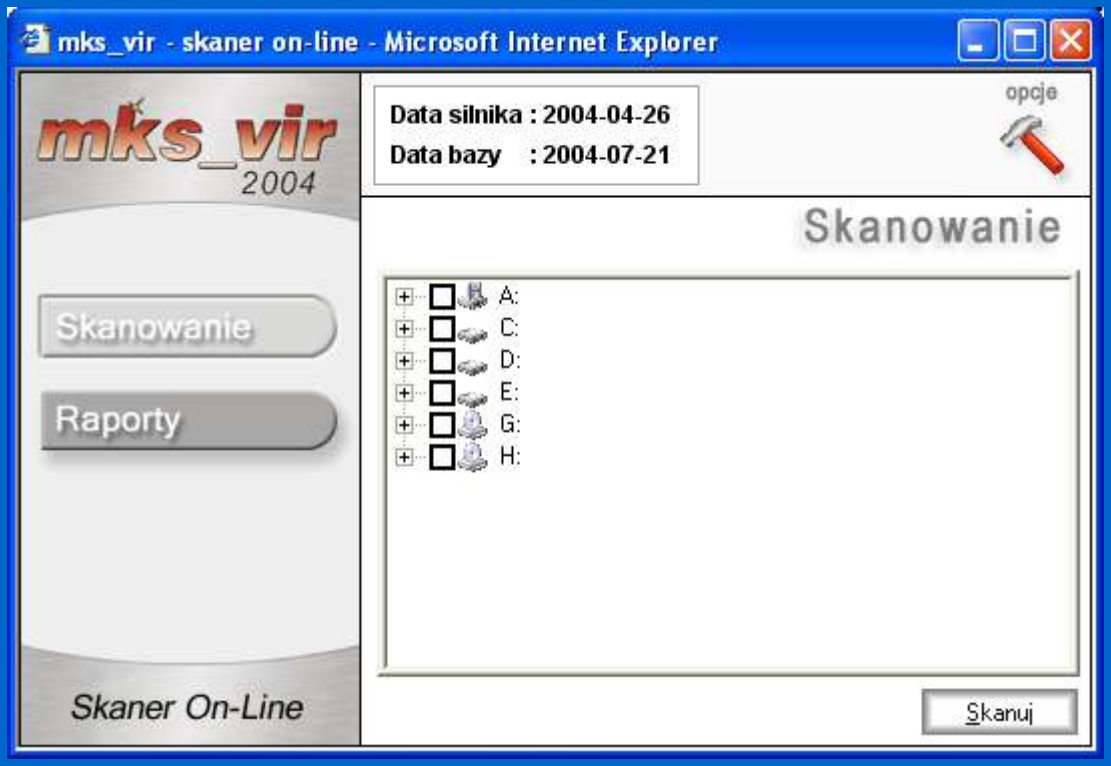

***Programy antywirusowe***
***Avast: http://www.avast.com/***

# Ochrona komputera




***Skanery antywirusowe – lista:***
***http://programy.57.pl/skanery,on-line.html***

# Ochrona komputera

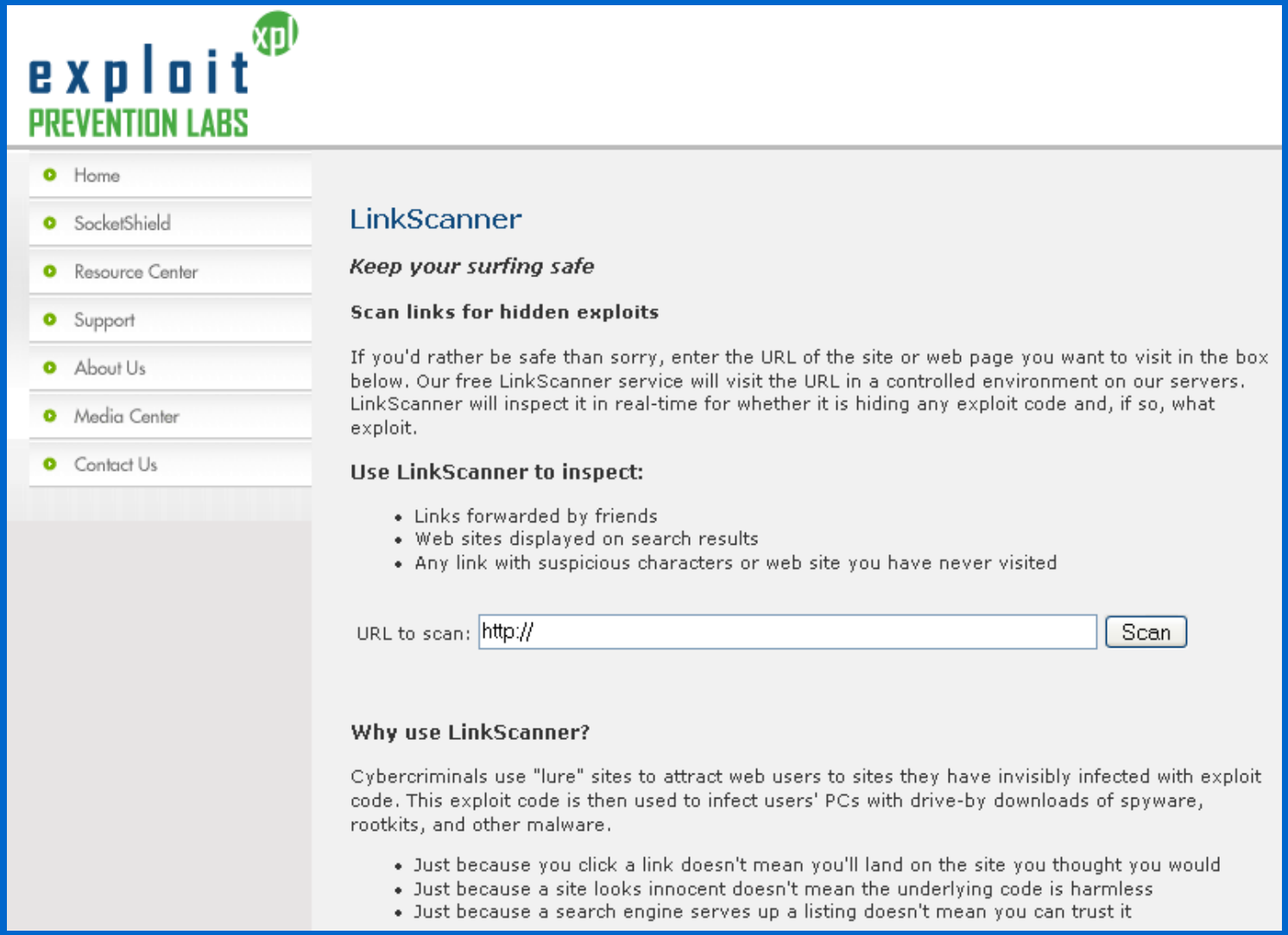



***Skanery antywirusowe on-linie***
***MKS: http://skaner.mks.com.pl/***

# Ochrona komputera

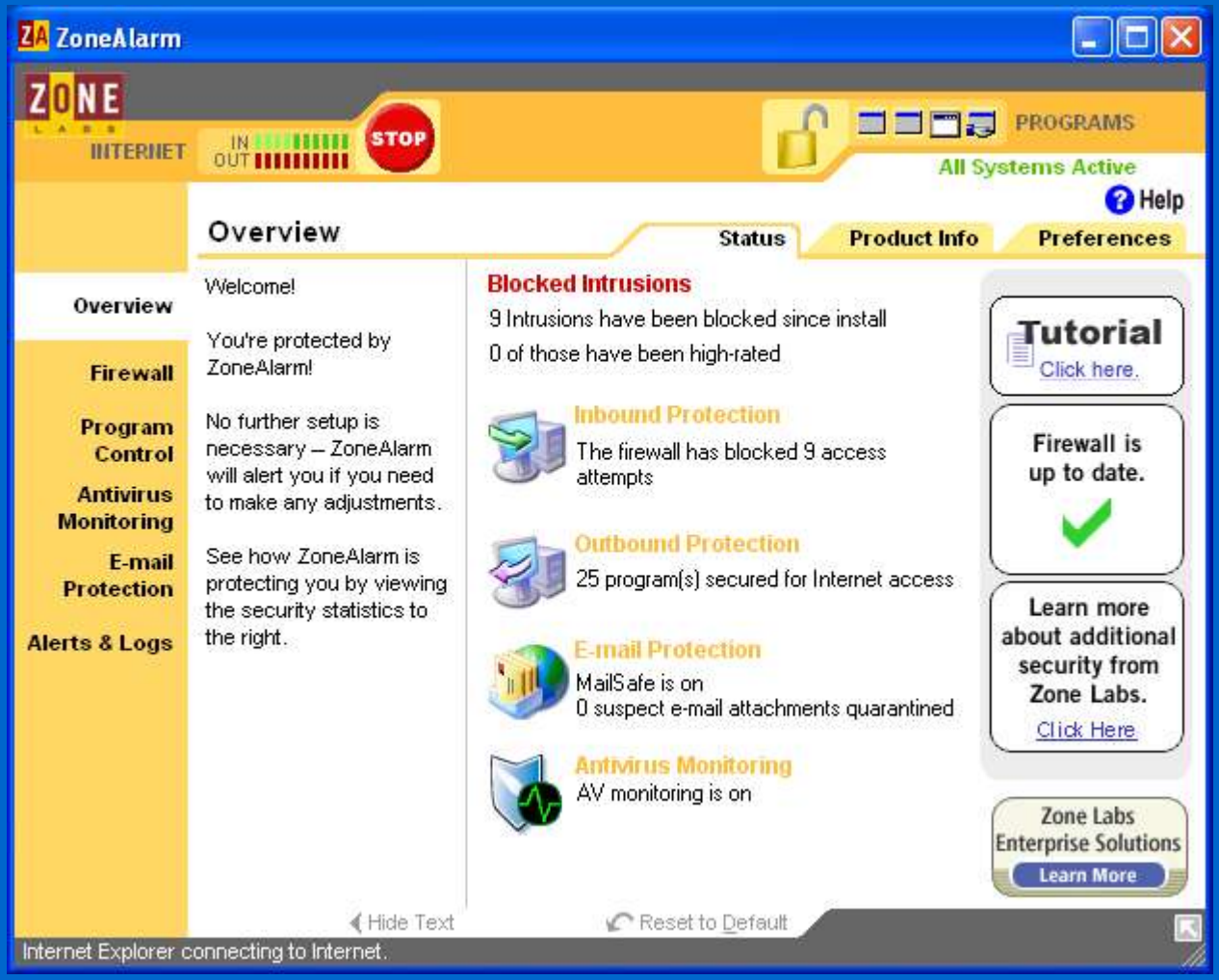

***Skanery antywirusowe on-linie***
***Symantec: http://security.symantec.com/***

# Ochrona komputera




***Link scanner***
***http://www.explabs.com/linkscanner/***

# Ochrona komputera




***Zapora ogniowa (Firewall)***
***ZoneAlarm: http://www.zonelabs.com/***

# Ochrona komputera


***Zapora ogniowa (Firewall)***
***Outpost Firewall: http://www.agnitum.com/***

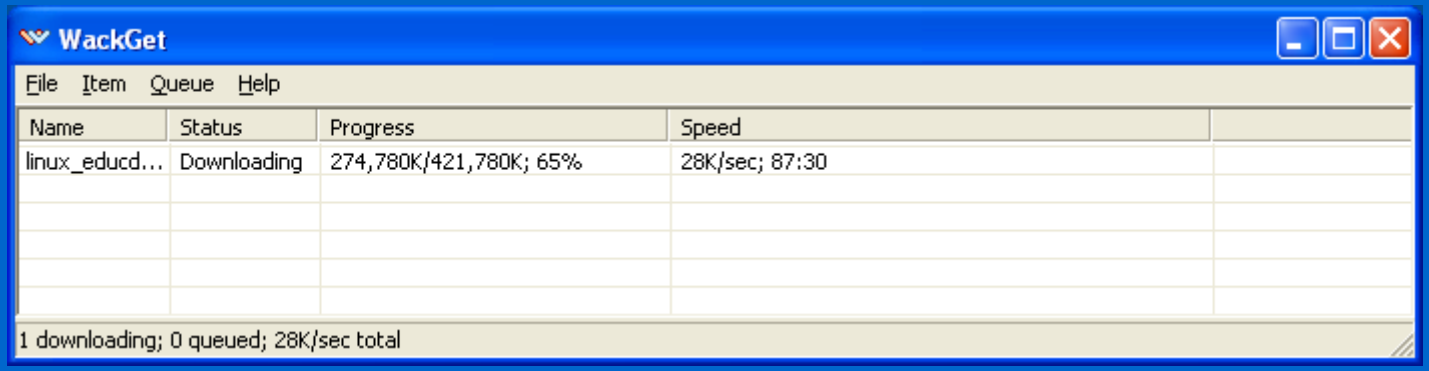
# Ochrona komputera


***Czyszczenie rejestrów***
***AdAware: http://www.lavasoftusa.com/software/adaware/***

# Ochrona komputera

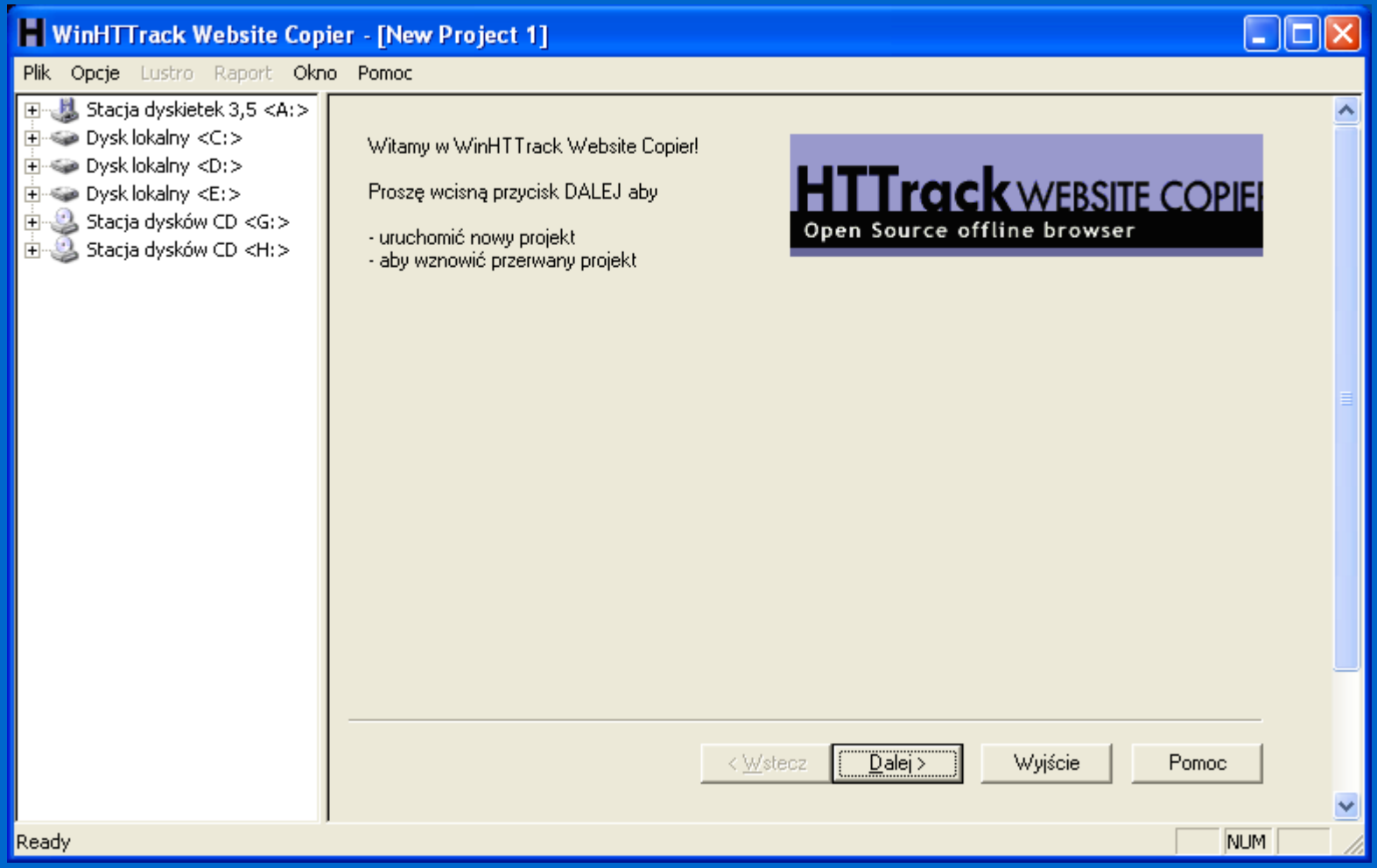

***Czyszczenie rejestrów***
***SpyBot: http://www.spybot.info/en/index.html***

# Narzędzia



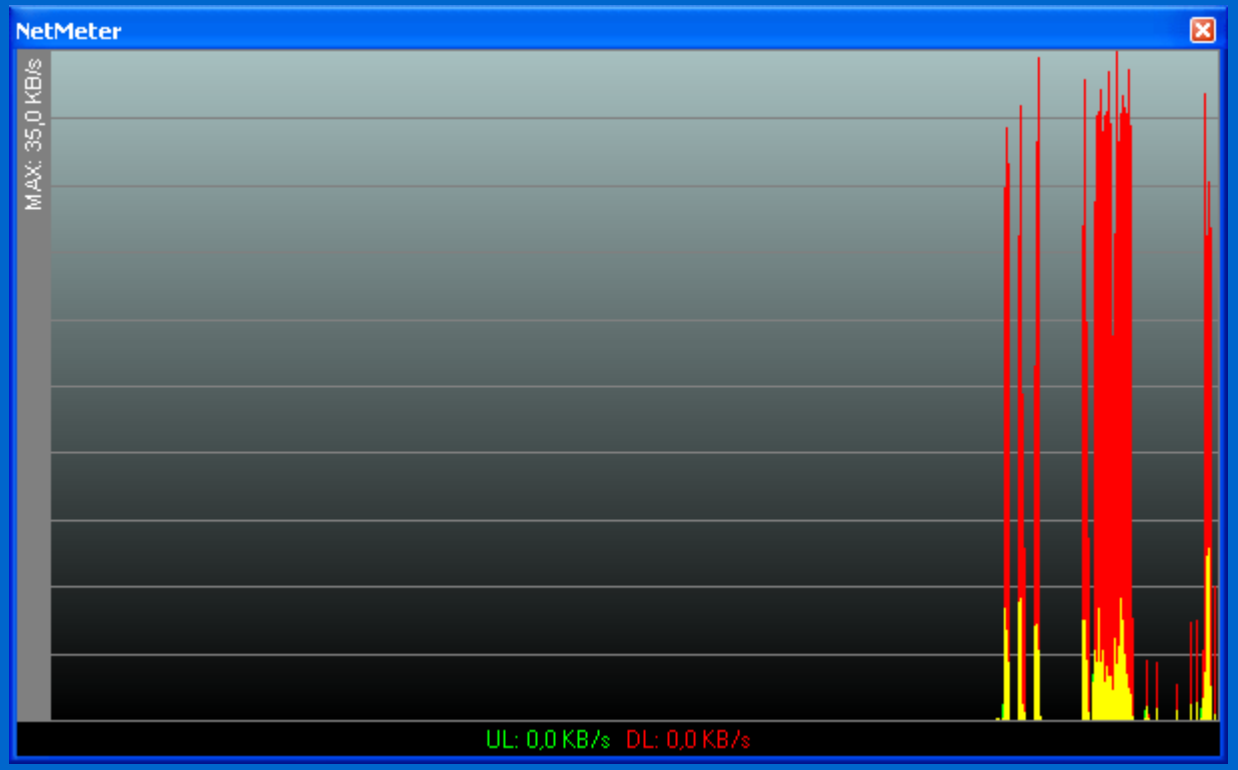

***Pobieranie plików***
***WackGet: http://www.spybot.info/en/index.html***

# Narzędzia




***Pobieranie plików***
***WinHTTrack: http://www.httrack.com***

# Narzędzia




***Monitoring sieci***
***NetMeter: http://readerror.gmxhome.de/***

# Internet i Prawo

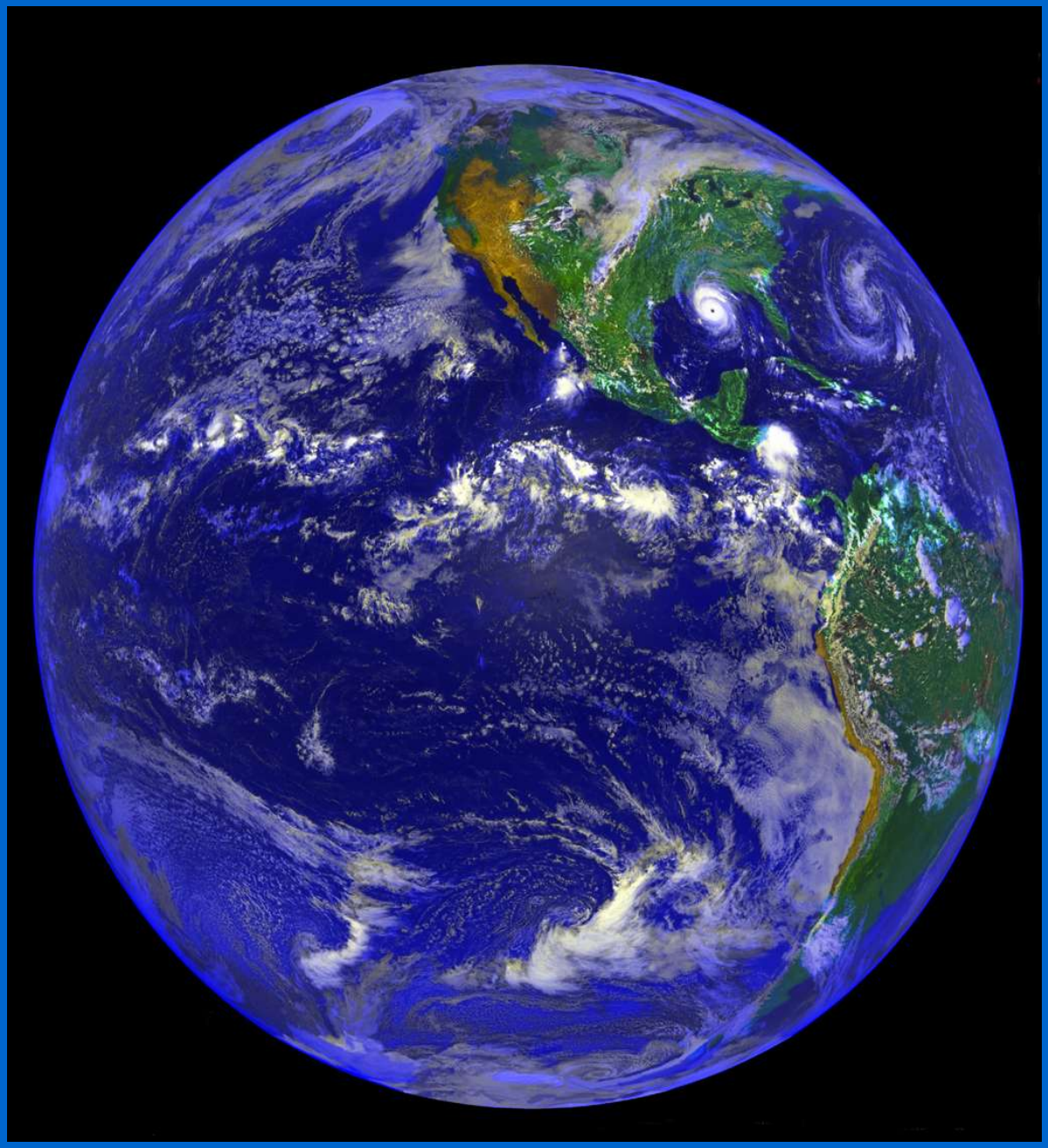
**Najczęstsze zagrożenia związane z Internetem, mające konsekwencje prawne dla użytkownika:**

- nielegalna wymiana plików muzycznych i filmowych
- pobieranie nielegalnego oprogramowania
- rozsyłanie spamu
- rozsyłanie wirusów
- włamania na strony internetowe (hacking)
- zakup za pośrednictwem Internetu kradzionych przedmiotów (najczęściej na aukcjach internetowych)

# Netykieta

**Netykieta -** to zbiór zasad przyzwoitego zachowania w Internecie, swoista etykieta obowiązująca w sieci.

Netykieta podobnie jak zwykłe zasady przyzwoitego zachowania nie są dokładnie skodyfikowane ani nikt nie zajmuje się systematycznym karaniem osób łamiących te zasady, jednak uparte łamanie zasad netykiety może się wiązać z różnymi przykrymi konsekwencjami jak np: odcięcie "niegrzecznego" osobnika od określonej usługi internetowej przez administratora danej usługi.



# Dziękuję za uwagę

Wojciech Sobieski

Olsztyn 2005