Zestaw

najważniejszych rad,
co robić,
a czego nie robić

dla #dzieciWsieci

CYFROWY

Poradnik Robić nie robić

cyfrowyskaut.pl

Drogi odbiorco,

z poniższego zestawu najważniejszych rad, dowiesz się, co robić, a czego nie robić. Kierujemy go głównie do dzieci i młodzieży.

Stosuj się do nich, aby:

- zadbać o swoje bezpieczeństwo w sieci;
- jak najlepiej wykorzystać technologię;
- uniknąć szkodzących ci konsekwencji.

Daj nam informację zwrotną, co lepiej wyjaśnić, poprawić, a czego jeszcze brakuje.

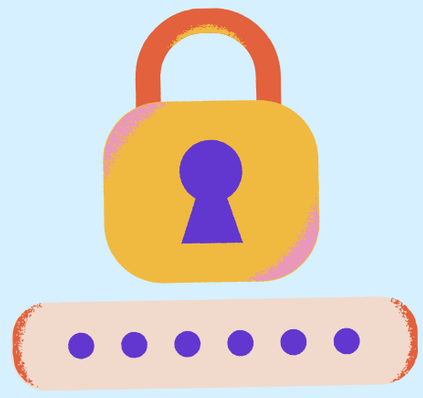
Napisz na ***info@cyfrowyskaut.pl***

Pamiętaj o tym, że:

- nie wszystko w sieci jest prawdą;
- ludzie nie zawsze mają dobre intencje;
- warto ograniczyć zaufanie do ludzi, informacji, narzędzi, serwisów internetowych;
- twój odbiorca wiadomości może mieć gorzej zabezpieczony telefon;
- nie masz wpływu na jakość bezpieczeństwa w miejscach, gdzie zostawiasz swoje informacje, zdjęcia, hasła i może to wypłynąć (być publicznie dostępne) bez twojej zgody i wiedzy;
- dobrze jest rozmawiać z dorosłymi, których znasz, są obok Ciebie, ufasz im, masz 100% pewności, że to oni (gdy kontaktujesz się online), znają się na technologii (lub radzą się kogoś kto się zna);
- to ty podejmujesz decyzje o jakości swojego bezpieczeństwa;

- to twoja decyzja, ile czasu przeznaczasz na oglądanie filmików, budowanie komuś statystyk czy zrobienie czegoś pożytecznego dla siebie i oglądanie filmów; dotyczących zainteresowań, pasji;
- im więcej sam się nauczysz, tym bardziej bezpieczniej będziesz korzystać z sieci;
- najlepszym sposobem na naukę siebie, jest nauka innych.

Bezpieczeństwo w grach



Rób:

- miej wyjątkowe (różne od innych) hasło;
- włącz dwuskładnikowe logowanie;
- kupuj tylko w oficjalnych sklepach;
- bądź miły dla innych;
- zgłaszaj oszustów i “hackerów”;
- określ maksymalny czas spędzony na graniu.

Nie rób:

- nie korzystaj z super, ultra promocji, o której wiesz z maila lub postu w mediach społecznościowych;
- nie miej takich samych haseł;
- nie wpisuj hasła na chacie gry;
- nie obrażaj, nie gróź innym graczom;
- nie podawaj innym hasła, haseł;
- nie wyłączaj antywirusa, żeby zainstalować grę;
- nie uruchamiaj cracków na komputerze;
- nie DDoSuj innych graczy.

CYFROWY Sk@ut ISSA POLSKA

Komunikatory internetowe

Rób:

- stosuj dwuskładnikowe logowanie;
- z graczami rozmawiaj tylko o grach;
- zawsze sprawdzaj czy login i hasło podajesz na prawdziwej stronie;
- zgłoś rodzicom, pedagogowi wszelkie prośby o:
  - spotkania z dorosłymi;
  - rozmowy wideo z nieznajomymi;
  - obejrzenie treści dla dorosłych;
  - podanie danych osobowych, adresu i statusu rodziny;
  - zachowanie znajomości w tajemnicy;
- zgłoś rodzicom, pedagogowi zawsze:
  - wymierzony w ciebie hejt, nienawiść;
  - zauważone obrazy krzywdzące Ciebie lub twoje otoczenie;

- konsultuj z rodzicami treści, których nie rozumiesz;
- miej odwagę zapytać dorosłych;
- weryfikuj znajomość online z kimś kogo znasz offline.

Nie rób:

- nie fałszuj tożsamości;
- nie obrażaj innych;
- nie wysyłaj złośliwych linków;
- nie klikaj w nieznane linki;
- nie wykonuj przelewu, jeżeli poprosi cię o to znajomy bez potwierdzenie z nim tego np. telefonicznie, że faktycznie to on napisał wiadomość;
- nie dziel się prywatnymi informacjami z osobami, których nie znasz z prawdziwego życia;
- pamiętaj, że niebezpieczne jest wysyłanie własnych zdjęć osobom, których nie znasz i nie masz pewności, co do ich tożsamości;
- wideorozmowa ze znajomymi poznanymi w sieci może być próbą wyłudzenia zdjęć, materiałów, danych;
- nie spotykaj się z dorosłymi poznanymi w sieci;
- nie podawaj haseł nigdy, nikomu, żadnym kanałem komunikacji.

TIK TOK i inne media społecznościowe

Rób:

- nagrywaj i publikuj piękne treści;
- oglądaj to, co sprawia ci prawdziwą radość;
- skonsultuj z dorosłymi czy wyzwania są bezpieczne.

Nie rób:

- nie czekaj na lajki, nie rób tego dla lajków;
- zanim weźmiesz udział w wyzwaniu, pomyśl czy jest to dla Ciebie i otoczenie bezpieczne;
- nie podejmuj się wyzwań, które polegają na okaleczaniu się, połykaniu rzeczy, których na co dzień się nie je, robieniu innych “wyjątkowych” rzeczy;
- nie nagrywaj i nie publikuj filmików, zdjęć, memów ośmieszających nikogo bez jego zgody - łatwo możesz wpaść w problemy z prawem.

Hejt, mowa nienawiści, nękanie

Rób:

- rozmawiaj z rodzicami, nauczycielami, dobrymi przyjaciółmi o krzywdzących cię treściach;
- zgłaszaj i raportuj komentarze krzywdzące innych;
- udzielaj konstruktywnej informacji zwrotnej;
- oceniaj zachowanie a nie osobę;
- wesprzyj offline osobiście koleżankę/kolegę, którzy są nękani w komentarzach.

Nie rób:

- nie oceniaj pod wpływem emocji;
- nie pisz emocjonalnych komentarzy;
- nie życz komuś czegoś złego;
- unikaj wycieczek osobistych, personalnie do osoby;
- nie odpowiadaj hejtem na hejt;
- nie daj się wciągać w dyskusje z trollami.

Prywatność w sieci

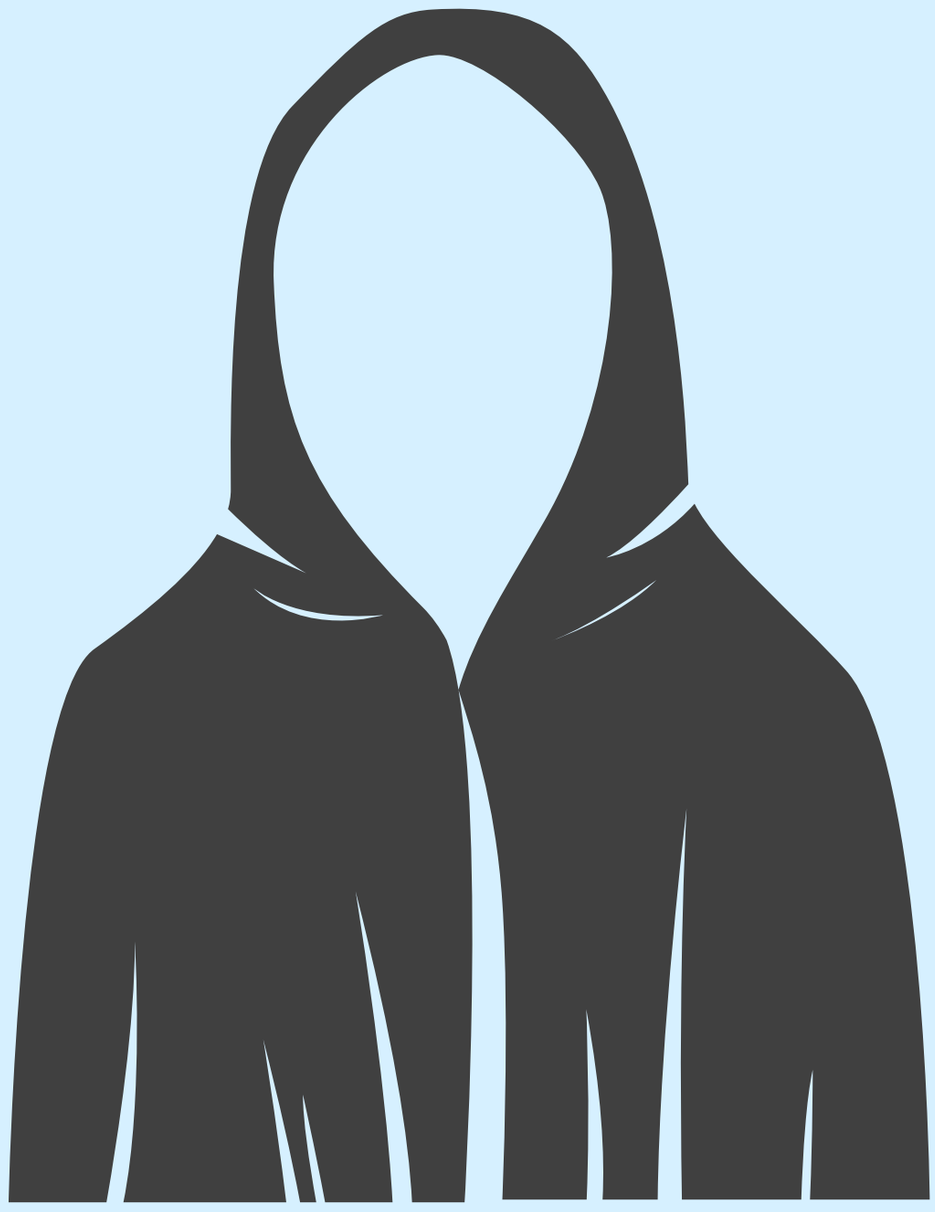
Rób:

- miej różne hasła do różnych portali/usług/urządzeń;
- używaj dwuskładnikowego logowania;
- używaj różnych adresów mail, do różnych usług (inny do rzeczy związanych ze szkołą, inny do zainteresowań);
- treści przeznaczone dla rodziny publikuj określając taką widownię;
- podczas rejestracji podaj tylko te informacje, które są niezbędne;
- szyfruj przechowywane dane;
- potwierdzaj informacje dwa razy;
- ogranicz widoczność swoich profili i świadomie zarządzaj dostępnymi informacjami;
- kasuj nieużywane profile;
- przećwicz odzyskiwanie hasła/ odzyskiwanie dostępu szczególnie do portali/profili, które są szczególnie dla Ciebie ważne;

Pamiętaj! Wszystko co raz zostało wrzucone do sieci zostanie tam na zawsze i może stać się dostępne publicznie.

Nie rób:

- nie podawaj danych na prośbę w mailu/komunikatorze;
- nie instaluj aplikacji z innych źródeł niż oficjalne;
- nie udawaj bycia anonimowym - anonimowość w sieci jest mitem;
- nie publikuj i udostępniaj publicznie danych, które nie powinny być publiczne;
- nie publikuj zdjęć swojej rodziny, domu.



Kariera zawodowa w IT

Rób:

- oglądaj materiały edukacyjne;
- naucz się uczyć;
- szukaj kolejnych materiałów;
- rób sobie notatki i naucz się robić je w jednym miejscu;
- znajdź wzorce do naśladowania;
- znajdź odpowiedź kto i za co może Ci zapłacić, jakie masz umiejętności;
- buduj portfolio swoich projektów.

Nie rób:

- nie marnuj czasu na treści, które nic nie wnoszą;
- nie patrz na branżę IT tylko z powodu “dużych pieniędzy”.

Zakupy w sieci

Rób:

- płać kartą płatniczą, ponieważ masz większe szanse na odzyskanie pieniędzy, jeśli zakup nie będzie skuteczny (procedura chargeback);
- szukaj AKTUALNYCH opinii o sklepie internetowym, o miejscu z opiniami;
- ustal limity dla przelewów, kart płatniczych, BLIKa (jednorazowej transakcji, dzienne, miesięczne);
- bądź bardzo podejrzliwy szczególnie do megapromocji;
- rób zakupy z dedykowanego konta (lub karty) z ograniczoną ilością pieniędzy.

Nie rób:

- nie podawaj danych karty płatniczej – numeru, kodu weryfikacyjnego, danych logowania do banku przez telefon, na komunikatorach internetowych, w linkach otrzymanych SMSem;
- bank NIGDY nie prosi o zainstalowanie jakiegoś oprogramowania, nie ma swoich programów antywirusowych.

Urządzenia (komputer, telefon)

Rób:

- rób i sprawdzaj kopie zapasowe;
- szyfruj urządzenia;
- zabezpieczaj hasłem ekran i nie udostępniaj go nikomu;
- jeśli chcesz coś komuś pokazać na telefonie, korzystaj z dostępu nadzorowanego uniemożliwiającego wyjście z aplikacji;
- aktualizuj każde oprogramowanie (programy, system operacyjny, przeglądarki i dodatki do przeglądarek);
- używaj tylko zaktualizowanych wersji systemu operacyjnego;
- instaluj oprogramowanie tylko z oficjalnych stron producenta;
- pracuj tylko na swoim komputerze, swoim profilu;
- pracuj na koncie użytkownika nie administratora;

- sprzedając, pożyczając komuś urządzenie wyczyść je z danych, przywróć do ustawień fabrycznych;
- używaj programów VPN korzystając z publicznych sieci WIFI;
- kiedy masz taką możliwość to korzystaj z własnego WIFI udostępnionego z telefonu;
- zadbaj o ochronę DNSów;
- z ograniczonym zaufaniem traktuj każdy pendrive;
- najlepszy program antywirusowy to ten zaktualizowany i działający.

Nie rób:

- unikaj logowania się korzystając z publicznych komputerów;
- nie instaluj pirackich programów, zawierają wirusy;
- nie wyłączaj programu antywirusowego, bo w instrukcji instalacji, używania jakiegoś programu była taka rekomendacja;
- nie pracuj na koncie administratora;
- nie ignoruj komunikatów programu antywirusowego;
- nie otwieraj załączników o wątpliwej zawartości (nieznanych), bo ktoś Cię ponagla lub o to prosi.

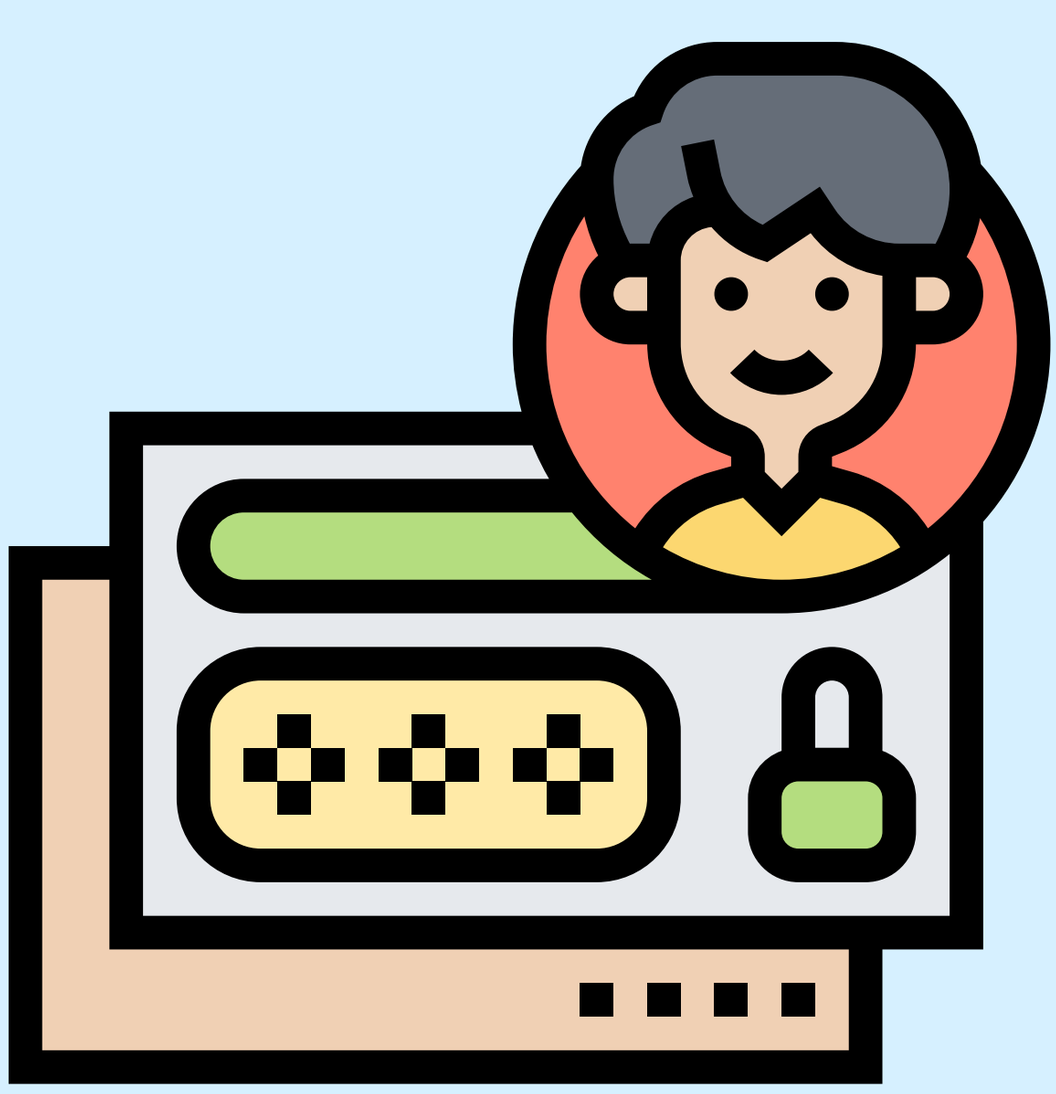
Hasła

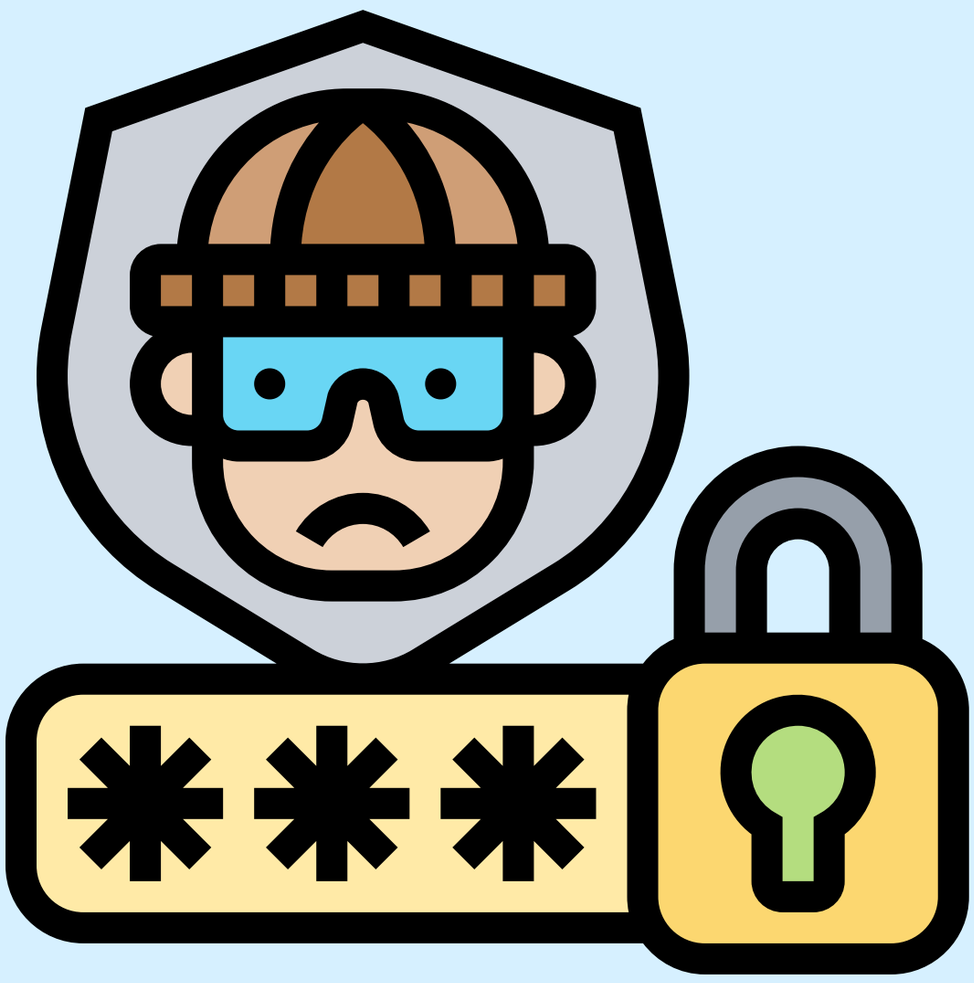
Rób:

- używaj różnych haseł do różnych usług (nie powtarzaj haseł między portalami);
- korzystaj z managerów haseł;
- używaj haseł wygenerowanych przez programy;
- stosuj bardzo długie hasła, które mogą być zdaniem (najlepiej bez spacji), przykładowo: ***Takie,sobie.2.Owce.w.lesie***;
- włącz drugi składnik logowania;
- włącz subskrypcję wycieków haseł, sprawdzaj czy hasła wyciekły na stronie https://haveibeenpwned.com/ oraz https://bezpiecznedane.gov.pl/;
- wyloguj się zawsze po pracy na nie swoim (obcym, szkolnym, publicznym) komputerze lub telefonie.

Nie rób:

- nie reaguj na wymuszenie zmiany haseł wysłane mailem i weryfikuj u źródła prawdziwość takiej informacji;
- nie przekazuj hasła nigdy nikomu pod żadnym pretekstem, a jedyny wyjątek to rodzic, który stoi obok ciebie;
- nie zapisuj haseł nigdzie poza zaufanymi managerami haseł (w na kartkach, w notatkach, plikach, nawet ukrytych).





Router domowy

Rób:

- aktualizuj urządzenie;
- wpisz silne hasło dla administratora urządzenia;
- stosuj długie i jednocześnie łatwe do podyktowania hasło do sieci WIFI;
- zabezpiecz WiFI standardem przynajmniej WPA2;
- wyłącz dostęp administracyjny z Internetu;
- zadania z gwiazdką*:
  - na starym routerze możesz używać aktualizowanego oprogramowania ***OpenWRT*** lub ***Tomato***;
  - zrób sieć dla gości i dla urządzeń ***IoT***;
  - udostępniaj rodzinie, znajomym dostęp do WIFi poprzez kod QR.

Nie rób:

- nie używaj urządzenia, którego producent już nie aktualizuje;
- sprawdzaj czasami czy adresy serwerów DNS są takie jakie zostały przez ciebie wpisane.

Portale społecznościowe

Rób:

- używaj silnych haseł i drugiego składnika uwierzytelnienia;
- dodawaj do grona znajomych tylko osoby, które znasz;
- weryfikuj, co publikujesz publicznie, a co tylko znajomym;
- aplikacje pobieraj tylko z zaufanych źródeł ***Google Play*** dla Android, ***App Store*** dla iOS i ***Microsoft Store*** dla Windows;
- ogranicz dostęp do informacji o sobie w ustawieniach prywatności;
- włącz powiadomienia o nowych logowaniach na twoje konto.

Nie rób:

- nie udostępniaj wrażliwych danych;
- nie publikuj zdjęć; które cyberprzestępcy mogą wykorzystać przeciwko tobie;
- nie używaj tego samego hasła w wielu portalach.

Fałszywe gry i inwestycje

Rób:

- uzgadniaj z rodzicem, jeżeli w grze lub na stronie jesteś proszony o wykonanie przelewu;
- weryfikuj reklamy;
- pobieraj gry tylko z zaufanych źródeł i od znanych wydawców.

Nie rób:

- nie ufaj gwarancji szybkiego pewnego zysku;
- nie pobieraj gier z linków od osób, które przed chwilą poznałeś w sieci;
- nie inwestuj bez konsultacji z dorosłymi;
- nie podawaj dalej.

Data dokumentu 20.06.2023

CYFROWY

Sk@ut

ISSA POLSKA

Poradnik Robić nie robić

cyfrowyskaut.pl

Daj nam informację zwrotną,
co lepiej wyjaśnić, poprawić,
a czego jeszcze brakuje.

info@cyfrowyskaut.pl

ISSA POLSKA