Elementarz dla rodziców

Dbaj o bezpieczeństwo dzieci w Internecie!

ins@fe

Partnerem jest: upc

SPIS TREŚCI

A. Jak należy korzystać z informatora?

Jeśli twoje plany dotyczą jednego roku, uprawiaj ryż.
Jeśli obejmują one okres 10 lat, zasadź drzewo.
Jeśli dotyczą całego życia, wykształć swoje dziecko.

chińskie przysłowie

Szanowni Rodzice i Opiekunowie,

Oddajemy w Wasze ręce informator poświęcony bezpieczeństwu w Internecie dzieci w wieku od 6 do 12 lat. Ta dydaktyczna publikacja została stworzona w przekonaniu, że nowoczesne technologie powinny łączyć, a nie dzielić pokolenia. Informator ten powstał przy współudziale Insafe – europejskiej sieci, której działalność koncentruje się na budowaniu świadomości o zagrożeniach, z jakimi mogą zetknąć się użytkownicy Internetu. Partnerem jest firma UPC, która przyczyniła się do powstania tych podręczników.

Powinniśmy udzielać naszym dzieciom wyraźnych wskazówek, jak należy się zachowywać: na placu zabaw, w piaskownicy, przy przechodzeniu przez jezdnię, ale także w Internecie. Brak zachowania należytej ostrożności w sieci może być dla dziecka równie niebezpieczny jak brak ostrożności w prawdziwym życiu.

Niniejszy informator został stworzony po to, by pomagać dzieciom w bezpiecznym korzystaniu z Internetu. Książka zawiera ponad pięćdziesiąt wskazówek i ćwiczeń, które pomogą Wam, Rodzice, przekazać dzieciom informacje na temat właściwego zachowania w sieci w sposób zabawny, interesujący i zachęcający je do myślenia. Informator zawiera:

- dwie broszury poświęcone bezpieczeństwu w sieci: część zawierającą materiały dla całej rodziny oraz przewodnik dla rodziców;
- praktyczne zasady przeznaczone dla wszystkich członków rodziny;
- certyfikat dla całej rodziny;
- zestaw naklejek;
- 12 kart do wycinania, opisujących różnego rodzaju sytuacje.

Zarówno broszura dla całej rodziny, jak i informator dla rodziców oznaczone są różnymi kolorami, aby podkreślić cztery główne tematy: Bezpieczeństwo, Komunikację, Rozrywkę i pobieranie plików z sieci i Cyberprzemoc. Informator dla rodziców zawiera komentarze i rozwiązania ćwiczeń zawartych w broszurze adresowanej do całej rodziny.

Z broszury dla całej rodziny mogą korzystać rodzice i dzieci. Cztery zagadnienia związane z bezpieczeństwem w sieci przedstawione zostały na przykładzie dwójki dzieci: Zosi i Kuby, ich rodziców oraz Julii – studentki informatyki i opiekunki rodzeństwa. Każdy z rozdziałów zawiera ćwiczenia dydaktyczne, quizy, złote zasady oraz przydatne linki.

Wskazówka: Przeczytajcie na głos opowiadanie zamieszczone na początku każdego rozdziału wspólnie z dziećmi, a następnie spróbujcie razem wykonać wszystkie polecenia. Na końcu każdego rozdziału znajdują się karty z opisami sytuacji, które pomogą w nawiązaniu rozmowy z dzieckiem na tematy poruszone w tekście. Ich zilustrowanie pozwoli Waszemu dziecku szybciej przyswoić potrzebną wiedzę.

Kiedy Wasze dziecko przeczyta już cały informator i wykona wszystkie zadania, postarajcie się, aby otrzymało nagrodę. Może to być certyfikat dla całej rodziny, który zostanie podpisany przez Was wszystkich. Możecie na nim umieścić Zasady Bezpiecznego Korzystania z Internetu. Dzieci mogą także udekorować swoje książeczki kolorowymi naklejkami emotikonek.

Wasze opinie na temat informatora są dla nas bardzo ważne. W razie jakichkolwiek pytań prosimy kontaktować się z lokalnym koordynatorem programu Insafe. Mamy nadzieję, że cała Wasza rodzina będzie się dobrze bawić, poznając Internet razem z naszym przewodnikiem!

Bezpiecznego serfowania!

Zespół Safer Internet,
www.saferinternet.pl

1. Ochrona oznacza bezpieczeństwo

KOMPUTER W DOMU

Komputer w domu może być świetnym narzędziem, służącym do nauki i rozrywki dla całej rodziny. Umieszczenie komputera w pokoju dziennym oraz określenie warunków korzystania z niego przez dziecko, łącznie z czasem, jaki dziecko może spędzić przed monitorem, sprawi, że najmłodsi będą korzystać z komputera w sposób racjonalny.

Pamiętajcie, że dzieci mogą korzystać z **Internetu** nie tylko w swoim domu, ale także w domach swoich kolegów i koleżanek, w kawiarenkach internetowych. Ważne jest, abyście wspólnie określili zasady bezpiecznego korzystania z Internetu, które dziecko będzie mogło stosować w każdym miejscu i o każdej porze.

ZABEZPIECZANIE KOMPUTERA

Możecie chronić swój komputer jedynie wówczas, gdy zdacie sobie sprawę z możliwych zagrożeń oraz gdy będziecie dysponowali podstawową wiedzą na temat zabezpieczeń. Połączenie zdrowego rozsądku z narzędziami technologicznymi ochroni Was i Wasze dzieci przed zagrożeniami płynącymi z sieci.

Częste czynności, takie jak korzystanie z **przenośnej pamięci** pendrive USB lub **CD-ROM-ów**, otwieranie **załączników** czy **pobieranie plików z sieci** mogą być obarczone pewnym ryzykiem. Odnosi się to przede wszystkim do złośliwych **programów komputerowych (malware/badware)**, stworzonych w celu uszkodzenia komputera, kradzieży danych osobowych czy narażenia użytkowników na przetwarzanie ich danych osobowych w niechciany przez nich sposób.

Ważne jest, aby dzieci nauczyły się rozpoznawać szkodliwe oprogramowanie: **wirusy**, **robaki**, **konie trojańskie** oraz **spyware**, a także wiedziały, jak rozpoznać symptomy infekcji komputera. Przekażcie dzieciom podstawowe zasady bezpieczeństwa, tj.:
- korzystanie z Internetu tylko na komputerze, w którym zainstalowane zostało aktualne oprogramowanie **antywirusowe** oraz program typu **anty-spyware**,
- zachowanie ostrożności w czasie otwierania załączników do e-maili, szczególnie tych otrzymanych od nieznajomych,
- zachowanie ostrożności przy pobieraniu programów z Internetu bądź korzystaniu z przenośnej pamięci czy CD-ROM-ów.

WALCZ ZE SPAMEM

Osiemdziesiąt procent e-maili krążących w Internecie to **spam** (niechciane wiadomości), które mogą oddziaływać na Wasze dziecko. Uczestniczenie w społeczności internetowej poprzez **grupy dyskusyjne**, **czat**, **forum**, **portale społecznościowe** oraz wypełnianie **formularzy on-line** może generować spam. W sieci działają specjalne programy, które wyłapują adresy e-mailowe, a następnie tworzą z nich listy mailingowe rozsyłające spam. Firmy zajmujące się tego rodzaju działalnością są często zlokalizowane w krajach, w których nie istnieją przepisy prawne zapobiegające wysyłaniu niechcianych e-maili!

E-maile wysyłane jako spam zawierają m.in. treści pornograficzne, informacje na temat środków farmaceutycznych czy podejrzanych transakcji finansowych. Spam może także rozprzestrzeniać złośliwe oprogramowanie. W większości przypadków takie wiadomości wysyłane są w nieuczciwych zamiarach. Poniżej przedstawiono kilka wskazówek, które pomogą ochronić rodzinę:

- Używajcie **filtrów antyspamowych**. Dostawca usług internetowych zazwyczaj oferuje usługę zablokowania spamu, którą należy aktywować w programie obsługującym Wasze konta e-mail. Skontaktujcie się z dostawcą usług internetowych w celu uzyskania szczegółowych informacji. Regularnie sprawdzajcie folder zawierający **spam**, aby upewnić się, że znalazły się tam tylko niechciane e-maile. Technika także się czasem myli, więc możecie stracić ważne informacje, które system mógł zakwalifikować jako spam.
- Nauczcie swoje dzieci, aby nie otwierały e-maili otrzymanych od nieznajomych. Spam prawie zawsze zawiera zaproszenia i załączniki. Pokażcie dzieciom, w jaki sposób można zablokować osobę wysyłająca spam, lub powiedzcie im, żeby zawsze kasowały podejrzane wiadomości bez ich otwierania.

SERFOWANIE PO SIECI

Nawet najmłodsze dzieci mogą czerpać korzyści z serfowania po Internecie, znajdą w nim treści rozrywkowe, edukacyjne odpowiednie dla ich kategorii wiekowej. W Internecie znajduje się jednak wiele stron zupełnie nieodpowiednich dla dzieci.

Wyszukiwarki są świetnym narzędziem do znajdywania potrzebnych informacji w sieci. To, co odnajdzie wyszukiwarka, zależy od słów-kluczy, które do niej wpiszemy. Błąd w pisowni lub słowa pokrewne odnalezione przez wyszukiwarkę mogą nas skierować do niechcianych i niebezpiecznych treści. Poniżej znajduje się kilka wskazówek, które pomogą dzieciom bezpiecznie serfować po Internecie:

- Utwórzcie oddzielne konto użytkownika dla Waszego dziecka, korzystając z **systemu operacyjnego** (np. Windows, Linuks, Mac OS X), w którym będziecie mogli aktywować **kontrolę rodzicielską**.
- Sprawdźcie, jakie opcje kontroli rodzicielskiej są dostępne w Waszej **przeglądarce internetowej** oraz w wyszukiwarce. Upewnijcie się, którą z opcji można aktywować w **ustawieniach rodzinnych**.
- Zaproponujcie dzieciom korzystanie z **wyszukiwarki** odpowiedniej dla młodych użytkowników sieci. Przykładami takich wyszukiwarek są http://dzieci.wp.pl, http://kids.yahoo.com oraz http://www.askforkids.com
- Dodajcie do **Ulubionych** (jedna z opcji w przeglądarce) adresy stron, na które Wasze dzieci wchodzą najczęściej. W ten sposób umożliwicie im przeglądanie ich ulubionych stron bez używania wyszukiwarki internetowej.

Oprócz aktywowania w przeglądarce i wyszukiwarce stron internetowych opcji pozwalającej na kontrolę rodzicielską, możecie także skorzystać z dodatkowego **oprogramowania filtrującego**, pozwalającego chronić osoby niepełnoletnie przed nieodpowiednimi dla nich stronami internetowymi. Poproście o poradę sprzedawcę bądź poszukajcie w Internecie wersji testowych takich programów. Pamiętajcie jednak, że żadne oprogramowanie nie zastąpi dziecku wskazówek udzielanych przez Was. Instalacja narzędzi może Wam dać złudne poczucie bezpieczeństwa, podczas gdy oprogramowanie także może się pomylić. Bardzo ważne zatem jest to, żeby Wasze dziecko kierowało się własną wiedzą i zdrowym rozsądkiem.

Zdarza się, że oprogramowanie służące do filtrowania treści w Internecie jest aż tak restrykcyjne, że blokuje zupełnie neutralne strony. Może np. uniemożliwić dziecku zebranie informacji na temat II wojny światowej, gdyż na stronach poświęconych tej tematyce jest opisana przemoc. Powinniście także pamiętać, że każdy filtr, który zainstalujecie, Wasze bystre dziecko może wyłączyć. Dzieci często są mistrzami w zacieraniu śladów swoich działań w sieci. Będziecie mogli się dowiedzieć o tym, co Wasze dziecko robiło w sieci pod Waszą nieobecność tylko wtedy, gdy sami nauczycie się korzystać z komputera i oprogramowania.

Wejdźcie na stronę projektu **SIP-Bench** (zobacz: Przydatne linki), powstałego przy udziale Komisji Europejskiej. W jego ramach przebadano ponad 30 programów do kontroli rodzicielskiej oraz programy antyspamowe w celu zbadania ich efektywności w ochronie dzieci w wieku od 6 do 16 lat przed szkodliwym wpływem różnego rodzaju aplikacji internetowych. W skład tych aplikacji wchodzą: **strony www**, wysyłanie i pisanie e-maili, **przesyłanie plików**, udział w czatach czy **komunikatory**. Zapoznajcie się również z testami programów filtrujących dostępnych w polskiej wersji językowej, które możecie znaleźć na stronie www.saferinternet.pl
http://www.saferinternet.pl/raporty/jak_skutecznie_filtrowac_zawartosc_internetu.html

Oprócz konieczności unikania szkodliwych treści powinniście wytłumaczyć dzieciom, że nie należy wierzyć we wszystko, co się przeczyta lub zobaczy w Internecie. W broszurze poświęconej zabawie dla całej rodziny zachęcamy dzieci, aby szukając informacji w sieci, weryfikowały je na co najmniej 3 stronach internetowych. Powinny także zawsze podawać źródło informacji, jeśli wykorzystują je np. do odrobienia pracy domowej.

ZŁOTE ZASADY DLA RODZICÓW „SIECIAKÓW"

- Upewnijcie się, że Wasz komputer jest chroniony przez firewall oraz oprogramowanie antywirusowe i anty-spyware'owe. Postarajcie się, aby oprogramowanie było na bieżąco uaktualniane i zwracajcie szczególną uwagę na ostrzeżenia, jakie generuje program. Sprawdźcie, czy Wasz dostawca usług internetowych oferuje oprogramowanie antywirusowe i anty-spyware'owe, z których moglibyście skorzystać.

• Korzystajcie z filtru spamu, który zainstalowany jest w programie obsługującym pocztę e-mail i nie udostępniajcie swojego adresu w sieci. Unikajcie e-maili od nieznajomych i skanujcie wszystkie załączniki, zanim je otworzycie.

• Upewnijcie się, że ustawione zostały funkcje kontroli rodzicielskiej w systemie operacyjnym, przeglądarce internetowej, wyszukiwarce i programie obsługującym pocztę e-mailową. Stwórzcie oddzielne konta użytkowników dla dzieci. Upewnijcie się, że zabezpieczenia chroniące Waszą prywatność są ustawione na najwyższy poziom (można je znaleźć w „opcjach" w pasku narzędzi w przeglądarce internetowej).

• Zastanówcie się nad skorzystaniem z dodatkowego oprogramowania filtrującego.

• Gdy Wasz komputer zacznie zachowywać się w dziwny sposób, może to oznaczać, że został zainfekowany. Wówczas należy się skontaktować z dostawcą usług internetowych lub z informatykiem. Oni powinni Wam udzielić informacji, co należy w danej sytuacji robić.

• Jeśli natkniecie się na niepożądane treści w Internecie, skontaktujcie się z internetową gorącą linią w Waszym kraju (zobacz: Przydatne linki).

• Kiedy tylko możecie, usiądźcie obok dziecka serfującego po Internecie. Jest to świetny sposób do nawiązania rozmowy i dodatkowo pozwala zwiększyć zaufanie dziecka do rodzica. Niech wspólna nauka stanie się Waszym wspólnym zadaniem.

• Pamiętajcie, że te zasady bezpieczeństwa odnoszą się zarówno do Was, rodziców, jak i do dzieci. Zachęćcie dziecko do tego, aby mówiło Wam o wszystkim, co je zaniepokoi w czasie korzystania z Internetu.

PRZYDATNE LINKI

Dzieci mogą wziąć udział w kursie na temat bezpieczeństwa w sieci, śledząc internetowe przygody Sieciaków:
http://www.sieciaki.pl

Kluczem do bezpiecznego serfowania po Internecie jest wiedza – powinniście wiedzieć, jakie ryzyko niesie ze sobą korzystanie z sieci oraz jak możecie chronić przed nim siebie i dziecko. Więcej informacji znajdziecie na stronie:
http://www.saferinternet.pl

Gdybyście w czasie serfowania napotkali treści, które mogą być niezgodne z prawem, możecie to zgłosić pod adresem:
http://www.dyzurnet.pl

SIP-Bench:
http://www.sip-bench.org/sipbench.php?page=home&lang=pl

2. Komunikowanie LoL ;-D

FRAGMENTY UKŁADANKI

Pamiętacie, jak ważne było dla Was utrzymywanie znajomości z osobami w Waszym wieku, gdy dorastaliście? Internet dostarcza wielu nowych możliwości do kontaktowania się z przyjaciółmi, oferuje zupełnie nowe sposoby uczestniczenia w życiu rówieśników. Życie towarzyskie Waszych dzieci odbywa się w dużej mierze przy użyciu nowoczesnych komunikatorów: poprzez e-maile, komórki, **Gadu-Gadu**, **Tlen**, **Skype**, **pisanie blogów**, korzystanie z portali społecznościowych (np. **Grono.net**, **Nasza-Klasa**). Obecni nastolatkowie wykorzystują nowoczesne technologie, by komunikować się w przestrzeni, którą uważają za prywatną i pozbawioną kontroli rodzicielskiej.

Rozdział poświęcony komunikacji wprowadza rodziców i dzieci w tematykę związaną z **danymi osobowymi**, **prywatnością**, pozytywnymi interakcjami międzyludzkimi w sieci. Przedstawiono w nim także sposoby zarządzania ryzykiem, do którego zaliczyć można kontakty z nieznajomymi. Zachowanie prywatności w sieci jest ściśle powiązane z **kontami** i **profilami** internetowymi. Aby komunikować się przez Internet, niezbędne jest założenie konta.

W świecie realnym mamy różnego rodzaju identyfikatory i karty: bankomatową, miejską, na basen etc., które zawierają dane osobowe. We wszystkich elektronicznych dokumentach podajemy te dane, które stworzą nasz profil użytkownika. Podobnie jest w Internecie: aby zaistnieć w sieci, musimy stworzyć swój profil, możemy jednak i powinniśmy upubliczniać tylko te dane, które chcemy, i tylko tym osobom, do których mamy zaufanie.

Ochrona prywatności polega na zarządzaniu informacjami na własny temat, którymi chcemy się podzielić z innymi, a nie na konfabulacji na własny temat i tworzeniu fałszywego obrazu siebie. Młodzi ludzie bardzo entuzjastycznie podchodzą do możliwości nieograniczonej kreacji w Internecie, jednak rzadko zdają sobie sprawę z konsekwencji takiego działania.

TWORZENIE PROFILU

Pierwszym krokiem w kierunku ochrony danych osobowych jest stworzenie bezpiecznego profilu. Powinniśmy najpierw ustalić, jakie informacje chcemy w nim zamieścić i jakie ustawienia prywatności zastosować.

Dobrym rozwiązaniem jest utworzenie kilku kont e-mailowych do różnych celów: do kontaktu ze znajomymi (tu możemy ujawnić imię i nazwisko), do czatu, forów dyskusyjnych, pisania lub czytania blogu (wtedy lepiej posługiwać się pseudonimami). Także dziecko zachęćcie do tego, aby wybrało nie tylko neutralny adres e-mail, ale także neutralną **nazwę użytkownika pojawiającą się na ekranie**. W ten sposób będziecie mieć pewność, że dziecko w czasie korzystania z czatu nie będzie używać adresu e-mail zawierającego jego pełne imię i nazwisko.

Nigdy nie udostępniajcie swojego **hasła**. Upewnijcie się, że Wasze dziecko wie, że dostęp do jego konta mogą mieć tylko zaufane osoby. Możecie także poprosić swojego syna lub córkę o to, aby podali Wam hasło do swoich kont, abyście mogli monitorować ich działania w sieci i zapewnić im ochronę.

Ustawienia prywatności profilu/konta w Internecie służą do określenia tego, czy chcecie być dostępni dla wszystkich użytkowników sieci, czy tylko dla wybranych, których znacie i z którymi chcecie się komunikować. Utworzenie profilu prywatnego oznacza, że sami zarządzacie swoją **listą kontaktów**. Pokażcie dzieciom, w jaki sposób akceptuje się kontakty z osobami znanymi ze świata realnego i jak dołącza się je do kontaktów bezpiecznych.

Jeśli Wasze dzieci korzystają z czatu, upewnijcie się, że:

- **czat jest moderowany**, gdy nie ma moderatora czatowanie nie jest bezpieczne;
- znają narzędzia pozwalające na ignorowanie bądź blokowanie uczestników czatu, z którymi nie chcą rozmawiać;
- wiedzą, gdzie na stronie internetowej znajduje się opcja pomocy i zgłaszania **problemów**, jeśli tylko się pojawią;
- zasady uczestnictwa w czacie są określone w sposób jasny i przejrzysty.

ZDJĘCIA I KAMERY INTERNETOWE

Dzieci powinny wiedzieć, że ich zdjęcia są ich prywatną własnością i że, opublikowane w sieci, mogą być rozpowszechnianie bez wiedzy właściciela i być źródłem manipulacji. Wysłane z komputera lub telefonu komórkowego, mogą pozostać w sieci nawet na zawsze! Wszyscy powinniśmy zachowywać ostrożność w czasie korzystania z **kamer internetowych**, a dzieci nie powinny się nimi posługiwać bez wiedzy i kontroli rodziców. Używanie kamer internetowych w trakcie czatów oraz w internetowych katalogach użytkowników kamer jest ryzykowne. Zarówno Wy, jak i Wasze dziecko, powinniście wysyłać zdjęcia cyfrowe jedynie do osób, które znacie i które darzycie zaufaniem. Zawsze należy poprosić o zgodę właściciela zdjęcia, zanim ja opublikujemy. Nie instalujcie dzieciom kamer internetowych w ich pokojach, bo mogą wówczas posługiwać się nimi bez Waszej wiedzy.

KONTAKT Z NIEZNAJOMYMI

Poznane w sieci osoby nie zawsze są tymi, za które się podają. Tak jak w rzeczywistości prosicie swoje dzieci, aby nie rozmawiały z nieznajomymi, tę samą zasadę powinniście stosować w odniesieniu do świata wirtualnego. Chodzi o bezpieczeństwo Waszych pociech.

Dzieci są ufne z natury, dopiero w czasie nabywania życiowych doświadczeń uczą się dystansu i zdrowej nieufności. Często zdarza się, że w sieci nawiązują bardzo bliskie relacje z nowo poznanymi osobami, bo te okazały im zrozumienie i zainteresowanie. Może się zdarzyć, że będą chciały spotkać się z taką osobą w świecie realnym i nie będą chciały (na prośbę wirtualnego „przyjaciela") poinformować Was o tym. Dzieci często nie są świadome niebezpieczeństwa, jakie niesie ze sobą takie spotkanie, i ignorują tego rodzaju zagrożenie. Wskutek tego stają się łatwymi ofiarami osób, które **uwodzą** dzieci w Internecie (ang. grooming). Badania Fundacji "Dzieci Niczyje" pokazują, że 45 % polskich nastolatków spotykało się ze "znajomymi" poznanymi w Internecie, a tylko 15 % rodziców tych nastolatków wiedziało o tym. Koniecznie porozmawiajcie na ten temat ze swoim dzieckiem i upewnijcie się, że będzie uważne i, co ważniejsze, każdorazowo poinformuje Was o zamiarze spotkania z osobą poznaną w Internecie.

Kluczem do wzajemnego zrozumienia jest dobra komunikacja.

NETYKIETA

Netykieta to zbiór zasad zachowania się w Internecie. Dzieci nie zdają sobie sprawy z tego, że zupełnie przypadkiem mogą kogoś obrazić. Niestety, niektórzy wykorzystują Internet i telefony komórkowe do dokuczania innym. Takie zachowanie nosi nazwę **cyberprzemocy** (ang. cyberbullying). Nawet co czwarte dziecko korzystające z sieci doświadczyło takiej przemocy (więcej informacji w rozdziale poświęconym temu zagadnieniu).

JĘZYK CZATU

Podczas czatu młodzi ludzie używają specjalnego języka składającego się z **emotikonek** i **akronimów**! W poniższej tabeli zamieszczono niektóre stosowane z nich.

Poniżej znajduje się przykładowa lista akronimów stosowanych w trakcie czatów. By uzyskać dodatkowe informacje, zobacz *"Przydatne linki"*

Polskie akronimy:

ATSD: A tak swoją drogą

AZS: Ale z drugiej strony

BP: Bardzo przepraszam

DoZo Do zobaczenia

JSM: Jak się masz?

komp: komputer

KWWO: Kończ waść! Wstydu oszczędź!

MZ: Moim zdaniem

MBSZ: Moim bardzo skromnym zdaniem

MSPANC: Mogłem się powstrzymać ale nie chciałem

NMZC: Nie ma za co

OCB: O co biega?

OIDP: O ile dobrze pamiętam

OIMW: O ile mi wiadomo

TSZS: Tarzam się ze śmiechu

ZGD: Z góry dziękuję

ZTCW: Z tego co wiem

Z/W Zaraz wracam

Angielskie akronimy:

KISS: Niech to będzie proste (ang. keep it simple, stupid)

BBL: Wrócę później (ang. be back later)

L8R: Później (ang. later, wymowa podobna do angielskiej wymowy eight(8))

IRL: W realu, w realnym świecie (ang. in real life)

LOL: Głośno się śmiejąc, będąc pod wrażeniem (ang. laughing out)

CU: Do zobaczenia (ang. see you)

CUL: Do zobaczenia później (ang. see you later)

NP: Nie ma problemu (ang. no problem)

CYO: Do zobaczenia w Siecie (ang. see you online)

OIC: O. widzę, rozumiem, (ang. oh, I see)

EGBOK: Wszystko będzie dobrze (ang. everything going to be ok)

F2F: Twarzą w twarz (ang. face to face)

GL: Powodzenia (ang. good luck)

HAND: Miłego dnia (ang. have a nice day)

TTYL: Porozmawiamy później (ang. talk to you later)

TY: Dziękuję (ang. thank you)

Wy także możecie stworzyć emotikonki, łącząc ze sobą różne znaki przestankowe i litery. Poniżej znajduje się kilka przykładów:

Uśmiech (z lub bez noska)	:) lub :-) dwukropek, (myślnik), nawias
Smutek (z lub bez noska)	:(lub :-(dwukropek, (myślnik), nawias
Mrugnięcie okiem (z lub bez noska)	;) lub ;-) średnik, (myślnik), nawias
Zdziwienie (z lub bez noska)	: o lub :-o dwukropek, (myślnik), mała litera o
Duży uśmiech (z lub bez noska)	:-D lub : D dwukropek, (myślnik), duża litera D
Wysunięty język (z lub bez noska)	: p lub :-p dwukropek, (myślnik), mała litera p

ZŁOTE ZASADY

• Sprawdzajcie, w jaki sposób Wasze dzieci spędzają czas w Internecie, poproście je, aby pokazały Wam, w jaki sposób porozumiewają się ze swoimi przyjaciółmi.

• Nauczcie dzieci, że swoją prywatność chroni się poprzez:

- stworzenie bezpiecznego profilu użytkownika, w którym aktywowane zostaną ustawienia dotyczące prywatności
- ochronę haseł
- kontaktowanie się i odpowiadanie na wiadomości wysłane jedynie przez osoby znane z rzeczywistości
- pytanie o zgodę rodziców na umieszczenie w internecie zdjęć swoich lub rodziny, domu, szkoły, itd
- dzielenie się danymi osobistymi, takimi jak numer telefonu, adres, nazwa szkoły, sporty, jakie uprawiają, tylko z osobami, które dobrze znają z rzeczywistości.

• Umieśćcie komputer w dużym pokoju, tak abyście mogli kontrolować aktywność dzieci w sieci.

• Wszyscy powinniście wiedzieć:

- jak odmówić zaakceptowania nowego kontaktu lub jak zablokować osobę z listy kontaktów
- jakie są zabezpieczenia oraz funkcje informowania o nieprawidłowościach występujących w trakcie korzystania z danej strony internetowej.

• Budujcie zaufanie, tak aby Wasze dzieci wiedziały, że mogą z Wami porozmawiać, jeśli popełnią jakiś błąd, oraz że zawsze wspólnie spróbujecie znaleźć rozwiązanie! Uczymy się na błędach!

PRZYDATNE LINKI

Kampania „Dziecko w Sieci" to działania na rzecz bezpieczeństwa dzieci i młodzieży w internecie. Więcej o samej kampanii oraz wiele pożytecznych porad dotyczących bezpieczeństwa najmłodszych użytkowników w sieci można znaleźć na stronie:
http://www.dzieckowsieci.pl

Helpline to projekt, w ramach którego świadczona jest pomoc w sytuacjach zagrożenia dzieci i młodzieży w Internecie:
http://www.helpline.org.pl.

Jeśli natknęliście się w sieci na nielegalne treści (pornografia dziecięca, rasizm, ksenofobia) – reagujcie! Zgłoście to w Dyżurnecie:
http://www.dyzurnet.pl

Raport Eurobarometr 2007, przedstawiający wyniki badań dotyczące korzystania przez dzieci z Internetu:
http://ec.europa.eu/information_society/activities/sip/eurobarometer

Wielki słownik akronimów:
http://emotka.net/slownik_akr/slownik_akr.php

3. Cyberprzemoc

PRZYPADEK PRZEŚLADOWANIA W SIECI

Możliwość komunikowania się przez Internet i telefony komórkowe daje wiele korzyści. Niestety, istnieje także pewne ryzyko – dzieci mogą otrzymywać oraz wysyłać wiadomości zawierające treści, które mogą ranić ich uczucia lub uczucia innych. Dlatego ważne jest, aby Wasze dzieci wiedziały, jak należy się zachowywać – one także nie są aniołkami ;-)

Cyberprzemocą jest wykorzystywanie nowoczesnych technologii komunikacyjnych i informatycznych do znęcania się, nękania i zastraszania pojedynczych osób lub całych grup. Może się to odbywać poprzez e-maile, czaty, wysyłanie wiadomości w czasie rzeczywistym, telefony komórkowe i inne nowoczesne narzędzia. W odniesieniu do gier internetowych możliwe jest zaatakowanie **awatara (wirtualnej postaci)** Waszego dziecka np. poprzez strzelanie do niego, kradzież jego **własności** czy zmuszanie go do zachowywania się w sposób, w jaki samo nigdy by się nie zachowało.

Zjawiskiem często zgłaszanym przez dzieci jest ujawnianie prywatnych informacji w miejscach publicznych, np. na forum lub stronie internetowej, publikowanie zdjęć. Tak samo jak **prześladowanie** w szkole czy na boisku, takie zachowanie nie może być akceptowane przez rodziców i nauczycieli, a dzieci powinny być czujne i gotowe zareagować w należyty sposób. W życiu realnym dziecko zna swojego prześladowcę, natomiast w świecie wirtualnym może on pozostać nieznany i wywołać znacznie większy lęk u dziecka. Osoby stosujące tego rodzaju przemoc często wysyłają groźby pocztą elektroniczną lub na telefon komórkowy wtedy, kiedy prześladowany się tego nie spodziewa.

Rolą rodziców jest takie wychowanie i edukacja swoich dzieci, aby te nie brały udziału w wirtualnym prześladowaniu innych. Dzieci powinny wiedzieć, jakie są ich prawa i za co są odpowiedzialne. Powinny również wiedzieć, że należy szanować prawa innych osób.

Zawsze należy być otwartym na rozmowę z dzieckiem, tak aby mogło powiedzieć o niepokojącej sytuacji. Uczcie je, jak z pożytkiem dla siebie i bez czynienia krzywdy innym korzystać z nowych technologii.

ZŁOTE ZASADY

• Nie dopuszczajcie do sytuacji, które mogą mieć szkodliwy wpływ na Wasze dziecko. Rozmawiajcie ze swoimi dziećmi tak, żeby wiedziały jak chronić swoją prywatność oraz szanować prywatność innych;

• Wasze dzieci powinny wiedzieć, że nie należy rozpowszechniać wiadomości, które mogą sprawić przykrość innym;

• Pomóżcie swoim dzieciom zrozumieć, jakie wiadomości i zachowanie może sprawić drugiej osobie przykrość i jak można temu zapobiec;

• Upewnijcie się, że dzieci wiedzą, jak można zablokować otrzymywanie e-maili od osób, które nie znajdują się na ich liście kontaktów;

• Zapisujcie obraźliwe wiadomości – być może będą stanowiły ważny dowód;

• Dowiedzcie się, jakie strategie przeciwdziałania cyberprzemocy wprowadzone zostały w szkole Waszego dziecka. Współpracujcie z innymi rodzicami i nauczycielami, aby przeciwdziałać prześladowaniom w świecie rzeczywistym i w sieci;

• Poznajcie środowisko Waszego dziecka – jego przyjaciół, ich rodziców, nauczycieli oraz kolegów i koleżanki z klasy;

• Zachęcajcie swoje dziecko do tego, aby było z Wami szczere, nawet jeśli zachowa się bezmyślnie – każdy ma prawo do popełniania błędów, a razem jest łatwiej je naprawić!

• Upewnijcie się, że dziecko wie, że to nie z jego winy ktoś mu dokucza.

PRZYDATNE LINKI

Jeśli Wasze dziecko: odwiedza niebezpieczne strony internetowe, otrzymuje niepokojące zdjęcia, wiadomości, podało swoje prywatne dane znajomym z Internetu, spotyka się z osobami poznanymi w Internecie, zbyt dużo czasu spędza przy komputerze, a Wy nie wiecie, jak z nim o tym porozmawiać i co zrobić, przeczytajcie porady zawarte na stronie:

http://www.helpline.org.pl

lub skontaktujcie się z konsultantem:

bezpłatna infolinia 0800 100 100

e-mail: helpline@helpline.org.pl

Strona ogólnopolskiej kampanii poświęconej bezpieczeństwu dzieci w Internecie:

http://www.dzieckowsieci.pl

4. Rozrywka i pobieranie plików z sieci

W SIECI NIE WSZYSTKO, CO SIĘ ŚWIECI, JEST ZŁOTEM

Internet to wirtualne miejsce, w którym można znaleźć różnego rodzaju rozrywkę, dokonać zakupów, pobrać akcesoria. W wielu przypadkach są to operacje odpłatne i to powinniście wyjaśnić swojemu dziecku. Na co dzień z pewnością nie kupujecie dziecku wszystkiego, co zobaczy w telewizyjnych reklamach czy na wystawie sklepowej, dlatego też nie powinniście na to pozwalać także w sieci. Muzyka, gry, **dzwonki** i inne akcesoria i usługi są najczęściej odpłatne i dziecko, które o tym nie wie, może je nieświadomie zamówić w czasie korzystania z Internetu.

Spróbujcie poserfować po Internecie razem z dzieckiem i pokażcie mu, że takie produkty jak **dzwonki**, **tapety**, **pliki MP3** czy **awatary** są najczęściej odpłatne, a informacja o kosztach jest napisana małym, ledwie widocznym drukiem. Unikniecie w ten sposób pułapek marketingowych, zastawianych w sieci. Poproście swoje dziecko, aby każdorazowo, gdy chce ściągnąć coś z sieci, informowało Was o tym.

Aby abonować jakąś usługę (płatną czy bezpłatną), zazwyczaj konieczne jest wypełnienie **formularza on-line**, zawierającego pytania o dane osobiste. Wypełniajcie takie formularze tylko wówczas, gdy wiecie, do czego mają być wykorzystane dane osobowe i postarajcie się odradzić dzieciom wypełnianie takich formularzy samodzielnie.

Wyskakujące okienka (ang. pop-up) często są wykorzystywane do sprzedaży różnych rzeczy w Internecie. Nie zawsze są one szkodliwe; zależy to od tego, na jakiej stronie – godnej zaufania czy nie – są zamieszczone. Niekiedy wyskakujące okienka służą do sprzedaży produktów lub wypełniania formularzy on-line, zbierających nasze dane osobowe. Nauczcie swoje dzieci, aby zamykały okienka, które nie pochodzą z wiarygodnego źródła, klikając w czerwony krzyżyk w prawym górnym rogu.

GRY W SIECI

Gry internetowe różnią się od starszych gier cyfrowych tym, że wykorzystują **połączenie internetowe**. Dzieci mogą grać w gry sprzedawane na płytach CD/DVD, na **stronach internetowych**, **konsolach** czy w telefonach komórkowych lub innych przenośnych urządzeniach.

Istnieje bardzo szeroka gama gier internetowych, począwszy od bardzo prostych, takich jak Pacman i Tetris, a skończywszy na wirtualnych grach w czasie rzeczywistym, w których może wziąć udział kilku uczestników jednocześnie. Wiele z gier zachęca uczestników do wchodzenia na strony poświęcone wirtualnym społecznościom graczy. Strony tego rodzaju mogą narazić dzieci na ryzyko związane ze spotykaniem się z nieznajomymi osobami w Internecie (zobacz rozdział poświęcony “Komunikacji”).

Gry mogą odegrać ogromną pozytywną rolę w rozwoju dziecka poprzez kształtowanie zachowań społecznych, umiejętność samodzielnego myślenia. Wiele z nich to gry ciekawe i interaktywne, które z powodzeniem mogą być wykorzystywane do celów edukacyjnych.

Jednak zauważyć należy, że nie wszystkie gry mają takie cechy. Powinniście mieć wpływ na to, w co gra Wasze dziecko, by mieć pewność, że są to gry odpowiednie i nie wpływają na Waszego syna lub córkę negatywnie.

PEGI online to ogólnoeuropejski system oceny gier internetowych, w którym gry sklasyfikowano pod względem wieku graczy i treści w nich zawartych. Przy pracach nad systemem udział wzięło kilkunastu producentów konsol, m.in. SONY (PlayStation), Microsoft (Xbox 360) i Nintendo (Wii, Nintendo DS) oraz wydawcy i twórcy interaktywnych gier z całej Europy. Czytajcie dokładnie opisy gier na pudełkach oraz wskazówki dotyczące wieku gracza, pamiętając jednocześnie, że każde dziecko jest inne i to Wy powinniście decydować, w jaką grę może grać.

ŚCIĄGANIE i UDOSTĘPNIANIE PLIKÓW A PRAWA AUTORSKIE ©

Młodzi ludzie często korzystają z Internetu jak z darmowej biblioteki filmów, gier i muzyki, które można pobrać, zagrać, obejrzeć i posłuchać. Do tego celu wykorzystują **sieci peer-to-peer** (w skrócie **p2p**), dzieląc się między sobą zasobami Internetu. Często jednak nie zdają sobie sprawy lub pomijają fakt, że rozrywka w Internecie ma swoich autorów, którzy mają prawo otrzymywać wynagrodzenie za wykorzystywanie ich dzieł.

Co jest, a co nie jest legalne w sieci?

Udostępnianie plików nie jest nielegalne, jeśli przesyłamy pliki, które sami stworzyliśmy. Ogólnie rzecz biorąc, **umieszczanie** i pobieranie plików z muzyką czy filmami bez zgody **właściciela praw autorskich** jest nielegalne na całym świecie (jednak każde z państw stosuje w tym względzie własne prawo autorskie). Oczywiste powinno być, że udostępnianie plików z muzyką czy z filmami jest nielegalne, oraz że powinno się zachować szczególną ostrożność w czasie korzystania z aplikacji obsługujących sieci typu **peer-to-peer**.

Czy to jest niebezpieczne?

Udostępnianie plików sprawia, że Wasz komputer narażony jest na niebezpieczeństwo, gdyż otwierane są porty (połączenia z Internetem), przez które może przedostawać się złośliwe oprogramowanie. Wskutek tego Wasz komputer może nieprawidłowo działać. Ponadto osoby nieupoważnione mogą mieć dostęp do Waszych danych osobowych i wysyłać spam lub wiadomości o treści niezgodnej z prawem.

Gdzie w sieci można znaleźć muzykę, którą można pobrać w sposób legalny?

Muzykę można pobrać za darmo w legalny sposób na setkach stron internetowych. Przykładem takich stron są strony zespołów muzycznych, gdzie najczęściej można posłuchać fragmentów utworów, dowiedzieć się więcej o dyskografii i planowanych koncertach.

ZŁOTE ZASADY

• Upewnijcie się, że korzystacie ze stron internetowych, z których legalnie można pobrać muzykę i filmy.

• Zachęcajcie dzieci do korzystania ze stron internetowych zawierających treści zgodne z prawem i zwróćcie ich uwagę na uproszczenia i półprawdy, jakie się mogą pojawiać w Internecie w różnych postaciach.

• Wyjaśnijcie dzieciom, jakie ryzyko niesie ze sobą pobieranie plików z sieci bez zachowania należytych środków ostrożności.

• Upewnijcie się, że Wasz komputer jest chroniony i że korzystacie z regularnie aktualizowanego oprogramowania antywirusowego.

• Nauczcie dzieci, że pliki internetowe, które chcą zapisać na twardym dysku, powinny być najpierw przeskanowane przez program antywirusowy.

• Zawsze czytajcie informacje na temat ochrony prywatności oraz pozostałe warunki umowy, zanim zainstalujecie cokolwiek na swoim komputerze. Sprawdźcie w Internecie , czy oprogramowanie, które chcecie pobrać, jest godne zaufania.

• Zamykajcie te z wyskakujących okienek, co do których nie macie zaufania, klikając w czerwony krzyżyk w prawym górnym rogu. Nigdy nie otwierajcie takich okienek.

DZIECI I GRY:

• Określcie zasady dotyczące czasu, jaki dzieci mogą spędzać, grając w gry komputerowe.

• Pozwólcie im grać na komputerze we wspólnym pokoju – tylko tam możecie mieć kontrolę nad czasem spędzanym przez dziecko przed komputerem.

• Obserwujcie, w co grają Wasze dzieci. Skoro pilnujecie ich podczas zabawy na podwórku, dlaczego nie robić tego, gdy grają w gry on-line?

• Porozmawiajcie o tematyce gry, w którą dziecko gra – sprawdźcie, czy ma ona walory

poznawcze i edukacyjne.

• Zanim kupicie swojemu dziecku grę, upewnijcie się, że jest odpowiednia dla jego wieku (można skorzystać z ogólnoeuropejskiego systemu klasyfikacji PEGI).

W czasie gier internetowych z innymi użytkownikami sieci:

• Poproście dziecko, żeby wchodziło tylko na strony internetowe, które mają surowe reguły uczestnictwa i na których obecni są moderatorzy.

• Ostrzeżcie dzieci, aby nie podawały swoich danych osobowych innym graczom.

• Ostrzeżcie dzieci, żeby nigdy nie spotykały się same z innymi graczami, a jeśli chcą pójść na takie spotkanie, któreś z Was powinno im towarzyszyć.

• Poproście dzieci, aby informowały Was o przypadkach przemocy w sieci, groźbach, wulgarnym języku używanym przez innych, lub innych nieodpowiednich treściach, które znajdą w Internecie.

• Nie pozwólcie, by Wasze dziecko grało w grę, która ma na nie zły wpływ. Możecie to zrobić, blokując dostęp do gry.

PRZYDATNE LINKI

Dowiedz się więcej na temat gier internetowych i o systemie ich klasyfikacji pod względem wieku:
http://www.pegionline.eu/pl/index/

Link do stron internetowych, na których można bezpiecznie i legalnie kupić muzykę:
http://www.pro-music.org

1. Ochrona oznacza bezpieczeństwo

KOMENTARZ DO ĆWICZEŃ

Połącz zdjęcie ze słowami: komputer, podkładka pod mysz, monitor, głośniki, kamera internetowa, drukarka, pamięć flash USB, mysz, płyty CD.

Ćwiczenie wprowadzające, które pozwala dzieciom na poznanie różnych części komputera oraz pozostałych urządzeń. Możesz dopasować to ćwiczenie do potrzeb dzieci, jeśli uznasz za stosowne.

Poproś swoich rodziców, aby wysłali do Ciebie e-mail wraz z załącznikiem lub wyślij go sobie sam. Potem wykonaj następujące polecenia: kliknij prawym klawiszem myszy w załącznik, a później zapisz go na pulpicie. Przejdź do pulpitu, kliknij prawym klawiszem myszy w dokument i kliknij w przycisk "Skanuj". Kiedy upewnisz się, że dokument nie zawiera wirusów, możesz go otworzyć. Pamiętaj: kliknij prawym klawiszem myszy, a następnie wybierz ZAPISZ – SKANUJ – OTWÓRZ.

Wyślij e-mail wraz z załącznikiem na adres swojego dziecka lub własny. Twoje dziecko powinno zastosować się do instrukcji w ćwiczeniu i zapisać dokument, klikając w niego prawym klawiszem myszy, jednocześnie nie otwierając załącznika. Gdy już plik zostanie zapisany na pulpicie lub w „Moich dokumentach", pokaż swojemu dziecku jeszcze raz, jak należy klikać prawym klawiszem myszy w dokument, aby go przeskanować, zanim zostanie otwarty. Dzięki powtarzaniu czynności dziecko lepiej zapamięta, co należy

zrobić, aby bezpiecznie otworzyć załącznik.

Skorzystaj z rady Julii i naucz się, w jaki sposób możesz zapisywać swój adres e-mail, kiedy chcesz go umieścić w sieci. Dzięki temu Twój adres e-mail nie zostanie automatycznie przechwycony i wykorzystany do wysyłania spamu. Na przykład cyberkot.nowak@adresemail.pl = cyberkot kropka nowak małpa adresemail kropka pl Aby poćwiczyć, opisz w ten sam sposób adresy e-mailowe członków Twojej rodziny: *Twój e-mail, e-mail Twojej rodziny, e-mail Twojej mamy, e-mail Twojego taty.*

Aby Twój adres e-mail nie był automatycznie przechwytywany przez oprogramowanie wykorzystywane do wysyłania spamu, opisz swój adres e-mail, ale nie podawaj go w pełnej postaci, np. zosia kropka nowak małpa wp kropka pl. Pozwól, aby Twoje dziecko poćwiczyło taki sposób zapisywania adresu e-mail jak przedstawiony powyżej. Pamiętaj jednak, aby Twoje dziecko nie publikowało swojego adresu e-mail w Internecie, a jeśli już to w formie nicku zamiast prawdziwego imienia (zobacz rozdział poświęcony komunikacji).

Aby pomóc Zosi zrozumieć to, o czym mówiła Julia, spójrz na listę ćwiczeń i zakreśl jedynie te, które można wykonać, będąc podłączonym do Internetu.

Twoje dzieci mogą nie wiedzieć, do których zadań konieczne jest połączenie z Internetem. Aby pisać na komputerze, nie musimy być podłączeni do sieci, jednak żeby wziąć udział w czacie, połączenie jest konieczne. Można słuchać muzyki na komputerze, gdy włożymy płytę CD czy też jeśli zapiszemy pliki z muzyką na twardym dysku. Możemy także słuchać muzyki bezpośrednio w sieci. Dzieci powinny zaznaczyć tylko te z zadań, do których konieczne jest połączenie z siecią.

Razem ze swoimi rodzicami wpisz w przeglądarkę internetową http://www.google.pl. Sprawdź, jakiego rodzaju informacje znajdują się pod hasłem Tyrannosaurus Rex i spróbuj się dowiedzieć, kiedy ten dinozaur żył na Ziemi. Spróbuj także znaleźć zdjęcie Tyrannosaurusa Rexa. Nie zapomnij sprawdzić informacji na co najmniej trzech stronach internetowych.

Wyrób u swoich dzieci nawyk wyszukiwania w sieci jedynie dobrych stron internetowych, przypominając im, aby nie ufały temu wszystkiemu, co znajdą w sieci. Przypomnij im, że szukając informacji na jakiś temat, trzeba przejrzeć przynajmniej trzy strony www i porównać informacje na nich zawarte. Ważne jest, by dzieci zawsze podawały źródło, z którego korzystały przy odrabianiu pracy domowej..

Razem ze swoimi rodzicami wpisz w przeglądarkę internetową http://www.google.pl. Następnie poszukaj informacji na dowolny temat, np. Tyrannosaurusa Rexa, i zapisz trzy strony internetowe, które uznasz za najbardziej interesujące, klikając w „dodaj do ulubionych" w górnym pasku narzędzi. Możesz również stworzyć swój własny folder. .

Zapisywanie i porządkowanie ciekawych stron internetowych w folderach (opcja w górnym pasku narzędzi) jest bardzo dobrym sposobem, aby dzieci w jak najmniejszym stopniu musiały korzystać z wyszukiwarek internetowych.

CZY MIAŁEŚ RACJĘ?

1: zabezpieczony 2: wirusa, nieznanych, pobierania, zainfekowanego 3: dziwnie 4: znasz, załączniki, tematy, spam 5: jednego, spamu 6: pierwszej, trzy , porównaj, każdy, opublikować 7: antywirusowy, anty-spyware 8: porozmawiaj, rodzicami 9: powiedz

PRZYKŁADOWE ROZWIĄZANIA PROBLEMÓW PRZEDSTAWIONYCH NA KARTACH

SYTUACJA 1. Nigdy nie serfuj po Internecie, jeżeli Twój komputer nie jest chroniony przez aktualne oprogramowanie antywirusowe oraz program antyszpiegowski. Jest to sytuacja, którą można porównać do granicy, na której nie ma strażników. Komputer może zostać zainfekowany przez szkodliwe programy, takie jak: wirusy, konie trojańskie, robaki czy program szpiegowski.

SYTUACJA 2. Miej oczy szeroko otwarte i uważaj na e-maile od nieznajomych osób, zawierające załączniki, jak również na e-maile typu „Wygraj milion dolarów". Najprawdopodobniej jest to spam! Spam może zainfekować komputer niebezpiecznymi programami, takimi jak wirusy, konie trojańskie, robaki czy program szpiegujący. Nie otwieraj takich e-maili. Możesz zablokować nadawcę takiej wiadomości, klikając prawym klawiszem myszki w e-mail i wybierając „zablokuj nadawcę"; możesz też po prostu skasować takie e-maile.

SYTUACJA 3. Kiedy szukasz informacji na dany temat w Internecie, nie polegaj od razu na pierwszej stronie, na którą wejdziesz. Sprawdź przynajmniej trzy różne strony i porównaj ze sobą znalezione informacje. Pamiętaj: każdy, kto ma dostęp do Internetu, może tworzyć i publikować informacje w sieci.

2. Komunikowanie LoL ;-D

KOMENTARZ DO ĆWICZEŃ

Jak bardzo **prywatne** są dla Ciebie informacje: Twój numer telefonu, Twoje imię, kolor Twoich włosów, Twój kraj, Twoja szkoła, Twój adres, imię Twojego zwierzaka, zawód Twoich rodziców, Twój adres e-mail, Twoje zdjęcia, Twój wiek?

Czy Twoje dzieci w taki sposób jak Ty postrzegają prywatność? Trzy z wykorzystanych kolorów oznaczają, że dane informacje są bardzo prywatne (kolor czerwony), dość prywatne (pomarańczowy) oraz że danych informacji nie traktujemy jako prywatne (zielony).

Pomóż Zosi stworzyć dobre hasło, wykorzystując poniższe wskazówki Julii.

Dobre hasło powinno być długie, zawierać przynajmniej 8 znaków (liczby, litery duże i małe, znaki przestankowe). Nigdy nie powinniśmy go podawać innym osobom.

Weź przykład z Zosi i stwórz swój bezpieczny profil. A następnie pokaż przykład profilu, który nie jest bezpieczny.

Pozwól, aby dzieci stworzyły bezpieczny profil, a następnie mniej bezpieczny profil, który zawierać będzie informacje prywatne. Przypomnij dzieciom, że utworzenie bezpiecznego profilu nie wystarczy, aby bezpiecznie korzystać z sieci. Przez cały czas korzystania z Internetu należy chronić swoją prywatność.

Spójrz na zdjęcie i napisz to, co mógłbyś powiedzieć na temat tej osoby.

Jakie informacje można odczytać ze zdjęcia? Dzieci często nie zdają sobie sprawy z siły obrazu.

Zgodnie z sugestią Zosi zastanów się nad trzema poradami, jakie "Kuba Czerwony Kapturek" mógłby usłyszeć od Julii, aby uchronić się przed „internetowymi wilkami"?

Upewnij się, że Twoje dzieci wiedzą, jakie ryzyko może nieść kontaktowanie się z nieznajomymi.

W jaki sposób chciałbyś, aby ludzie traktowali Ciebie w sieci? (1….. 2….. 3…..)

Upewnij się, że Twoje dzieci wiedzą, że powinny odnosić się z szacunkiem do innych użytkowników sieci.

ZŁAM KOD: Poznaj znaczenie niektórych z najbardziej popularnych akronimów, łącząc je z ich znaczeniem.

Dowiedz się, co oznaczają akronimy, sprawdzając ich znaczenie w rozdziale „Komunikowanie".

Użyj kombinacji klawiszy na klawiaturze do oznaczenia poniższych emotikonek: Uśmiech – Smutna twarz – Mrugnięcie okiem – Zdziwienie – Szeroki uśmiech – Wysunięty język.

Aby uzyskać dodatkowe informacje, przejdź do rozdziału pt. „Komunikowanie".

CZY MIAŁEŚ RACJĘ?

1: profil 2: prywatności, odpowiedzialny 3: obcymi, powiedz 4: Netykieta 5: emotikonka 6: hasło, przestankowe 7: tajemnicą 8: nie 9: znam

PRZYKŁADOWE ROZWIĄZANIA PROBLEMÓW PRZEDSTAWIONYCH NA KARTACH

SYTUACJA 4. Kiedy korzystasz z Internetu, Twój profil i informacje, które o sobie podajesz, mogą dotrzeć do dziesiątek, setek, tysięcy, a nawet milionów ludzi. Dlatego ważne jest, abyś był ostrożny, podając informacje na swój temat. Podawaj dane osobowe jedynie tym osobom, które dobrze znasz ze świata realnego i którym możesz zaufać.

SYTUACJA 5. Tomek prawdopodobnie podał swoje hasło do skrzynki e-mailowej koledze, który postanowił w jego imieniu wysłać nieprzyjemne maile. Nigdy nie podawaj nikomu swoich haseł, chyba że nie masz nic przeciwko temu, aby inni ludzie czytali Twoje e-maile i podawali się za Ciebie!

SYTUACJA 6. Spotkanie z osobą nieznajomą jest złym pomysłem. Jeśli naprawdę sądzisz, że możesz zaufać osobie poznanej w Internecie, która chce się z Tobą spotkać, powiedz o tym swoim rodzicom i poproś, aby jedno z nich poszło z Tobą na takie spotkanie. Nikt, kto ma uczciwe zamiary, nie będzie miał nic przeciwko temu. Może to być problemem jedynie dla tych, którzy mają coś do ukrycia.

3. Cyberprzemoc

KOMENTARZ DO ĆWICZEŃ

Wymyśl logo i hasło "Tygodnia przeciw cyberprzemocy"

Zachęć dziecko do kreatywnego wykorzystania całej strony.

Tak jak Kuba podaj pięć powodów, dla których ktoś mógłby dostać „czerwoną kartkę".

Porozmawiaj z dziećmi na temat zachowania, którego one same nie akceptują.

CZY MIAŁEŚ RACJĘ?

1: fair, psują 2: Rozmowa 3: powód 4: cyberprzemoc 5: Blokuję 6: dobrze 7: odpowiadam

PRZYKŁADOWE ROZWIĄZANIA PROBLEMÓW PRZEDSTAWIONYCH NA KARTACH

SYTUACJA 7. Takiego korzystania z telefonu na pewno nie można zaakceptować. Zawsze traktuj innych w taki sposób, w jaki ty sam chciałbyś być traktowany. W takiej sytuacji zawsze porozmawiaj ze swoimi rodzicami lub z inną osobą dorosłą, której możesz zaufać.

SYTUACJA 8. Kuba powinien powiedzieć swojemu koledze, że niewłaściwe zachowanie osoby, która go niepokoi, nie jest spowodowane jego zachowaniem. Nie powinien odpowiadać na wiadomości od osoby, która go nęka. Powinien je zachować jako dowód, który będzie mógł pokazać rodzicom bądź nauczycielom. Kuba powinien także porozmawiać na ten temat ze swoimi rodzicami, którzy mogą go wesprzeć, aby mógł pomóc swojemu koledze.

SYTUACJA 9. Netykieta to zbiór zasad zachowania w Internecie. Jesteśmy pewni, że wiesz już wystarczająco dużo, aby móc pomóc Zosi w tym zadaniu.

4. Rozrywka i pobieranie plików z sieci

KOMENTARZ DO ĆWICZEŃ

Otwórz swoją ulubioną wyszukiwarkę internetową. Wpisz „darmowe dzwonki" lub „darmowe gry" i zobacz, jakie otrzymasz wyniki wyszukiwania. Sprawdź kilka stron internetowych.
Czy natrafiłeś na jakieś pułapki?

Ćwicz dalej wpisując słowa kluczowe w wyszukiwarkę i sprawdź, czy na otrzymanych stronach www nie kryją się jakieś pułapki marketingowe. Zwróć uwagę, w jaki sposób w hasłach reklamowych omijane są informacje, które napisane zostały małym drukiem.

Jaka jest Twoja ulubiona gra komputerowa? Czy znają ją Twoi rodzice? Opowiedz im o niej, a potem poproś, aby napisali jej krótki opis. Czy mieli rację? Ile punktów byś im dał w skali od jednego do dziesięciu? Rodzic wpisuje krótki opis ulubionej gry dziecka. Dziecko rysuje obrazek z gry

Czy rzeczywiście wiesz, w jakiego rodzaju gry grają Twoje dzieci w Internecie, i czy wiesz, jaka jest ich ulubiona gra? Pozwól im Cię sprawdzić!

CZY MIAŁEŚ RACJĘ?

1: za darmo 2: formularze 3: kupić 4: nielegalnymi 5: krzyżyk 6: ignorować 7: prywatność 8: dzielić się, sam 9: pobieraj

PRZYKŁADOWE ROZWIĄZANIA PROBLEMÓW PRZEDSTAWIONYCH NA KARTACH

SYTUACJA 10. Większość plików z muzyką i filmami, które znajdują się w Internecie, to nielegalne kopie. Poza tym strony internetowe, na których ludzie dzielą się muzyką i filmami, mogą zawierać szkodliwe oprogramowanie, takie jak wirusy, konie trojańskie, robaki czy spyware. Najlepiej by było, gdyby Zosia wybrała odpowiedź b lub c. Oczywiście pobranie jej ulubionej piosenki ze strony internetowej, której można zaufać i która zawiera legalne pliki z muzyką, kosztować będzie znacznie mniej niż zakup płyty. Musiałaby zapytać swoich rodziców o pozwolenie.

SYTUACJA 11. Niektóre usługi oferowane w Internecie są darmowe, jednak dzwonki, tapety, pliki MP3, awatary itd. bardzo rzadko dostępne są bezpłatnie. Jeśli Kuba przeczyta dokładniej stronę internetową, zauważy informacje małym drukiem na temat prawdziwych kosztów oferowanej usługi. Dzwonki, quizy, gry, itd. to skuteczny sposób zachęcenia ludzi do skorzystania z tzw. darmowych usług, które w rzeczywistości takie nie są.

SYTUACJA 12. Kuba powinien pamiętać o tym, że kiedy gra w Internecie z nieznanymi osobami, nie powinien podawać nikomu swoich danych, takich jak: nazwisko, miejsce zamieszkania, numer swojej szkoły. Powinien także mówić rodzicom w jakie gry gra i nigdy nie powinien bez zgody rodziców pobierać gier z Internetu, ponieważ może to stanowić zagrożenie dla domowego komputera.

D. Słowniczek

Adres e-mail: wirtualne miejsce, do którego dostarczane są wiadomości e-mail. Adres e-mail składa się z dwóch części oddzielonych od siebie symbolem @.

Akronim: to skrót, na który składają się pierwsze litery danego słowa lub wyrażenia. Akronimy wykorzystywane są w rozmowach na czatach w celu szybszej komunikacji z drugą osobą. Przykładami akronimów są LoL, CU, BTW (zobacz rozdział poświęcony komunikowaniu).

Alarm: to małe okienko pojawiające się na ekranie, które przekazuje Ci informacje bądź ostrzega, że wykonanie danej operacji może być szkodliwe. Okienka tego rodzaju mogą się pojawić, gdy będziesz otwierał e-mail lub też kiedy Twój komputer zostanie przeskanowany przez system antywirusowy.

Antywirus: program komputerowy, którego celem jest identyfikowanie, izolowanie, blokowanie i niszczenie wirusów oraz złośliwego oprogramowania. Program antywirusowy skanuje pliki w celu znalezienia wirusów, a następnie lokalizuje pliki, które mogły zostać zainfekowane.

Autor: to osoba, która jest twórcą danego dzieła literackiego, filmu, oprogramowania, itd. Wszystko co zostało stworzone przez autorów, podlega ochronie prawnej i nie może być w sposób nielegalny powielane i rozpowszechniane.

Awatar: to profil użytkownika w świecie wirtualnym oraz w grach internetowych, przedstawiony za pomocą nazwy użytkownika i jego zdjęcia, ikony czy też trójwymiarowej postaci.

Blog: to krótka wersja pamiętnika internetowego. Jest to strona internetowa uaktualniana każdego dnia przez jedną osobę lub grupę osób o nowe teksty, zdjęcia, pliki wideo lub linki.

Blogowanie: czynność pisania lub uaktualniania informacji zawartych w blogu.

CD-ROM: akronim angielskich słów „compact disc read-only memory". Jest to płyta, na której nie można nic nagrać, zawierająca informacje, które nadają się do odczytu jedynie w komputerze. Na płytach CD-ROM często sprzedawane jest oprogramowanie komputerowe.

Cookie (ciasteczko): to identyfikator, jaki strona internetowa może przydzielić użytkownikowi. Przeglądarka internetowa zapamiętuje otrzymywane cookie i pozwala stronie je sprawdzać przy kolejnych wizytach. Dzięki temu można łatwo identyfikować użytkownika i tworzyć dostosowane dla niego strony. Ma to duże znaczenie w przypadku dokonywania zakupów w Internecie. W przypadku odrzucenia cookie, niektóre ze stron mogą przestać poprawnie działać.

Crack: czynność kopiowania w sposób nielegalny oprogramowania poprzez łamanie kodu zabezpieczającego oprogramowanie przed nielegalnym kopiowaniem.

Cracker: osoba, która nielegalnie i ze złymi intencjami włamuje się do innych komputerów.

Czat room (chat room, pokój czatowy): to najczęściej strona www pozwalająca na komunikowanie się z innymi osobami w czasie rzeczywistym. Ludzie z całego świata spotykają się w czat roomach, aby korzystając z klawiatury porozmawiać na różne tematy. Jeżeli Wasze dziecko korzysta z czat roomu, upewnijcie się, że taki czat room przeznaczony jest dla dzieci w jego wieku oraz że rozmowy są kontrolowane przez moderatorów.

Czat: jednoczesne komunikowanie się z drugą osobą korzystającą z Internetu za pomocą pisemnych wiadomości. W tym celu wykorzystywane są przeglądarki internetowe i komunikatory internetowe takie jak Gadu-Gadu, GoogleTalk, AIM, Skype, MSN.

Dane osobowe: wszelkiego rodzaju informacje związane z daną osobą. Jeżeli ktoś chce zapisać nasze dane osobowe, musimy wiedzieć do czego ich potrzebuje.

Dzwonek: dźwięk jaki wydaje telefon komórkowy, zanim zostanie odebrana rozmowa przychodząca. Istnieje szeroka gama różnych dzwonków i muzyki, które można pobrać na telefon, najczęściej po uiszczeniu opłaty.

E-mail (poczta elektroniczna): to rodzaj pisemnej komunikacji w sieci, pozwalającej na wysyłanie wiadomości razem z załącznikami takimi jak teksty, zdjęcia oraz pliki audio i wideo.

Emotikonka: obraz, ikonka, które niosą ze sobą uczucia bądź emocje, np. uśmiech. Symbolami stosowanymi do tworzenia emotikonek są symbole umieszczone na klawiaturze, znaki przestankowe oraz innego rodzaju gotowe symbole, z których najczęściej korzystamy w czat roomach, korzystając z komunikatorów internetowych czy też wysyłając wiadomości tekstowe z telefonu komórkowego.

Filtr antyspamowy: rodzaj aplikacji, której celem jest niedopuszczenie do przesyłania spamu pocztą e-mail.

Filtr rodzinny: program, którego celem jest kontrola dostępu do informacji lub usług internetowych, wykorzystywany do ostrzegania użytkownika o niebezpiecznych stronach www i do ich blokowania. Filtr zapamiętuje również odwiedzane strony i pozwala na kontrolę czasu dostępu do komputera i Internetu. Filtry mogą być zainstalowane na pojedynczych komputerach, a także na serwerach oraz np. w telefonach z dostępem do Internetu.

Firewall: rodzaj sprzętu (zainstalowanego w routerze) bądź rodzaj oprogramowania (zainstalowanego na

naszym komputerze), którego celem jest zablokowanie dostępu niepożądanych osób (np. hackerów) do danych zgromadzonych na komputerze.

Flaming: wrogie i obraźliwe zachowanie w stosunku do innych użytkowników sieci. Ma ono miejsce zazwyczaj w przypadku czatów (ang. Internet Relay Chat – IRC), a niekiedy występuje także w e-mailach.

Folder spamu: miejsce w e-mailowej skrzynce odbiorczej, w którym znajdują się e-maile uważane przez nas za spam.

Folder: to jednostka w systemie porządkowania plików, zawierająca kilka plików i/ lub inne katalogi. Foldery, które zawierają zazwyczaj kilka plików, wykorzystywane są do porządkowania informacji zawartych w plikach.

Formularz (formularz internetowy): sformatowany dokument zawierający puste pola, które należy wypełnić tekstem. Formularz elektroniczny może już zawierać wpisany tekst lub należy wybrać go z rozwijanej listy. Po złożeniu formularza dane w nim zawarte są wysyłane automatycznie do bazy danych.

Forum: internetowa grupa dyskusyjna, której członkowie mają podobne zainteresowania i wymieniają się poglądami na różne tematy.

Freeware: oprogramowanie dostępne za darmo, na co zgodę wyraził właściciel praw autorskich.

Gra komputerowa: gra stworzona przez informatyków, w którą można grać na komputerze. Gra internetowa (on-line) to gra, w którą można grać jedynie wówczas, gdy połączymy się z Internetem. Gry online umożliwiają interakcję między graczami.

Gra internetowa dla dużej liczby graczy (MMORPG Massively-Multiplayer Online Role Playing Game): gra on-line, przedstawiająca zazwyczaj trójwymiarowy świat, w którym setki graczy przyjmują role fikcyjnych lub historycznych bohaterów i wspólnie przeżywają przygody, często walcząc z potworami.

Grooming: to działania osoby dorosłej, która przy użyciu czat roomów (i innych środków komunikacji dostępnych w Internecie) stara się nakłonić dziecko do kontynuacji znajomości w formie spotkania w świecie rzeczywistym, z intencją jego seksualnego wykorzystania.

Grupa dyskusyjna: zobacz definicję słowa forum.

Hacker: osoba włamująca się do zabezpieczonych systemów komputerowych, łamiąca kody zabezpieczające (zobacz „cracker"). W kręgach informatyków terminem tym określa się osobę będącą entuzjastą komputerów, zdobywającą wiedzę, lecz nie czyniącą świadomie szkód.

Hasło: tajny ciąg liter, znaków i liczb umożliwiający dostęp do komputera, dokumentu, konta lub programu. Służy jako zabezpieczenie przed dostępem do naszego komputera i danych nieupoważnionym osobom (zobacz rozdział pt. „Komunikowanie").

Hotline: telefoniczne bądź internetowe wsparcie dla osób, które zgłaszają strony internetowe zawierające szkodliwe bądź nieprawdziwe treści. Hotline muszą posiadać ściśle określone procedury przyjmowania zażaleń. Wspieraniem hotline'u zajmuje się rząd, firmy, organizacje i stróże prawa. W Polsce w ramach projektu Saferinternet.pl działa hotline Dyżurnet .pl (www.dyzurnet.pl).

Infolinia: dostępna w wielu krajach usługa e-mailowa bądź telefoniczna, koordynowana przez organizacje zajmujące się pomocą dzieciom bądź też przez krajowe punkty kontaktowe różnego programu Insafe. Pozwala ona dzieciom zgłaszać informacje na temat niezgodnych z prawem i szkodliwych treści w sieci oraz informować na temat ich negatywnych doświadczeń związanych z korzystaniem z technologii informatycznych.

Internet: ogólnoświatowa i ogólnodostępna sieć połączonych ze sobą komputerów, pozwalająca na transmisję danych i wymianę plików. Obejmuje mniejsze sieci krajowe, akademickie, biznesowe oraz rządowe, pozwalające na korzystanie z usług takich jak przekazywanie informacji, wysyłanie e-maili, uczestniczenie w czatach czy też przesyłanie plików.

Junk e-mail (spam): niechciane, prawie jednakowe e-maile, wysyłane do nas z wielu skrzynek pocztowych. Często w ten sposób wysyłane są materiały reklamowe.

Kamera internetowa: kamera służąca do przesyłania obrazów i dźwięków za pomocą Internetu. Wykorzystywana jest w czasie czatu, wysyłania wiadomości w czasie rzeczywistym czy też w czasie wideo-konferencji. Kamery internetowe to kamery cyfrowe, które nieustannie bądź w pewnych odstępach czasu wysyłają obraz na serwer.

Katalog: jednostka służąca do porządkowania dokumentów i plików w komputerze, wykorzystująca do tego celu foldery. Katalogi znajdują się m.in. w folderach takich jak „Moje dokumenty" czy „Moje obrazy".

Komunikacja w czasie rzeczywistym (ang. instant messaging): rodzaj natychmiastowej komunikacji elektronicznej pomiędzy dwoma lub większą liczbą użytkowników. Wysyłanie wiadomości w czasie rzeczywistym pozwala na kontaktowanie się jednocześnie z kilkoma osobami. Jeżeli osoby znajdujące się na Twojej liście kontaktów są on-line, użytkownik danego rodzaju komunikatora internetowego jest o tym automatycznie informowany.

Konto: służy do identyfikacji Twojej osoby, kiedy korzystasz z komputera, lub z różnego rodzaju usług internetowych. W tym celu powinieneś ustalić swoją nazwę użytkownika oraz hasło.

Kontola rodzicielska: zobacz definicję ustawień rodzinnych

Koń trojański (trojan): złośliwy program, który może zostać zainstalowany na Twoim komputerze, kiedy będziesz wykonywał z pozoru nieszkodliwe operacje, takie jak np. granie w gry. Trojany nie rozprzestrzeniają się na komputerze, lecz poszukują danych lub je niszczą. Mogą one również skasować lub wykraść informacje zapisanie na twardym dysku komputera.

Kosz: katalog zlokalizowany na naszym komputerze, w którym znajdują się usunięte pliki, zanim zostaną całkowicie skasowane. Należy regularnie usuwać stare i nieprzydatne pliki z kosza, aby zwolnić miejsce na twardym dysku, czyli miejscu gdzie zapisywane są wszystkie dokumenty dostępne na naszym komputerze.

Kradzież tożsamości: kradzież danych osobowych danej osoby (np. imienia i nazwiska, daty urodzenia, numeru karty kredytowej) w celu wykorzystania ich w sposób niezgodny z prawem.

Link: odnośnik do dokumentu, który umieszczony jest w sieci (np. strona internetowa, dokument tekstowy, zdjęcie). Klikając w link automatycznie otworzysz nową stronę internetową. Pliki tekstowe mają zazwyczaj kolor niebieski i są podkreślone, mogą być jednak w każdym kolorze i nie zawsze muszą być podkreślone. Zdjęcia mogą także służyć jako linki do innych stron internetowych.

Lista kontaktów: zbiór kontaktów wykorzystywanych przez programy obsługujące pocztę e-mail oraz komunikatory internetowe, gry czy też telefony komórkowe. Do listy kontaktów można dodawać, usuwać lub odrzucać nowe osoby.

Malware (badware): skrót od angielskich słów „malicious software" (pol. złośliwe oprogramowanie), odnoszący się do oprogramowania mającego na celu zniszczenie dokumentów zapisanych na komputerze bez informowania o tym właściciela komputera. Malware obejmuje wirusy, robaki, konie trojańskie, spyware, nieuczciwe oprogramowanie typu adware oraz inne szkodliwe dla naszego komputera oprogramowanie.

Manipulowanie: proces zmiany zdjęcia, pliku lub ilustracji w sposób jawny lub ukryty. Obecnie istnieje wiele narzędzi, które służą do zamiany treści danej strony internetowej czy danych, co skutkować może niechcianymi konsekwencjami.

MP3: to plik z muzyką zapisany w specjalnym formacie. Plik MP3 jest mniej więcej 10 razy mniejszy niż oryginalny plik audio, a jakość dźwięku nie odbiega od jakości odbioru płyty CD. Z racji swojego małego rozmiaru i dobrej jakości dźwięku, pliki MP3 stały się bardzo popularnym sposobem przechowywania muzyki zarówno w komputerach, jak i różnego typu przenośnych odtwarzaczach.

Nazwa użytkownika (nazwa ekranowa): synonim imienia użytkownika pojawiający się na monitorze. Określa on użytkownika danej usługi internetowej i jest wybierany przez użytkownika sieci. Używany jest w listach kontaktowych, czat roomach. Jeżeli dobrze wybierzemy swój nickname, możemy chronić swoją anonimowość w sieci.

Net (Sieć): skrót od słowa Internet.

Netykieta: zbiór zasad zachowania się w Internecie.

Nickname (nick): zobacz Nazwa użytkownika.

Osprzęt (hardware): części składowe komputera. Zaliczyć do nich możemy płytę główną, twarde dyski oraz pamięć RAM, które często określane są terminem komponentów. Na osprzęt składają się także monitory, klawiatury, drukarki, i inne urządzenia, tzw. peryferia.

P2P (ang.peer-to-peer) jeden ze sposobów wymiany plików w sieci, pozwalający osobom podłączonym do sieci na wymianę plików poprzez ich pobieranie i wysyłanie jednocześnie. Ze względu na charakter większości wymienianych plików (nielegalne kopie muzyki, filmów i oprogramowania), sieci P2P są postrzegane jako potencjalne źródło naruszeń praw autorskich i zagrożeń, takich jak wirusy i malware.

Pamięć przenośna, pendrive, pamięć Flash-USB: pojemna pamięć przenośna z wtyczką USB. Pamięć przenośna zajmuje zazwyczaj niewiele miejsca, jest lekka i łatwo ją przenosić z miejsca na miejsce. Można na niej m.in. zapisywać i kasować pliki takie jak dokumenty, zdjęcia.

Pasek narzędzi: zestaw ikon i przycisków będących częścią interfejsu programu. Pasek narzędzi to stale widoczny i łatwy w użyciu zbiór ikon, pozwalający nam na wykonywanie pewnych funkcji w danym programie.

Plik komputerowy: zbiór danych (tekst, grafika, dźwięk), które zapisywane są na komputerze pod swoją własną nazwą. Pliki komputerowe to w dzisiejszym świecie odpowiednik dokumentów papierowych, które znajdowały się w biurach i w bibliotekach.

Pobierać (ściągać, downloadować): czynność odnosząca się do procesu jakim jest kopiowanie pliku z Internetu do komputera.

Połączenie internetowe: połączenie, którego używają użytkownicy sieci, aby korzystać z Internetu. Są różne metody połączenia z Internetem jak: łącza stałe (operatorzy telewizji kablowej, sieci osiedlowe) połączenia bezprzewodowe (WiFi, komórkowe GPRS/EDGE/3G, łącza satelitarne), linie telefoniczne (dial-up i xDSL).

Pornografia dziecięca: pornografia dziecięca jest pod względem prawnym definiowana różnie w różnych krajach. Jedna z definicji określa terminem pornografii dziecięcej zdjęcia, obrazy, filmy, które w widoczny sposób przedstawiają osobę małoletnią w trakcie czynności seksualnej.

Port: część komputera służąca do połączenia komputera z innym urządzeniem. Porty mogą być zarówno wewnętrzne, jak i zewnętrzne. Porty wewnętrzne łączą ze sobą twardy dysk lub sieć, podczas gdy porty

zewnętrzne łączą urządzenia peryferyjne, takie jak drukarka czy klawiatura, z komputerem.

Portale społecznościowe (ang. social networking sites): witryny (portale) internetowe pozwalające na wymianę poglądów oraz rozmowę na temat wspólnych zainteresowań członków danej wspólnoty. Każdy z członków posiada swoje konto i może korzystać z różnego rodzaju narzędzi internetowych, takich jak np. umieszczanie w sieci zdjęć, dokumentów, wysyłanie wiadomości czy też uczestniczenie w czatach. Korzystanie z wielu portali społecznościowych jest zabronione dla dzieci poniżej 13 roku życia, a liczne portale społecznościowe posiadają funkcję tworzenia bezpiecznych profili użytkowników.

Prawa autorskie (copyright): prawa danej osoby do pomysłu, dzieła lub informacji. Symbol „©" jest ogólnie przyjętym znakiem oznaczającym prawa autorskie.

Procesor: nowoczesny zminiaturyzowany układ scalony, będący częścią komputera. Jego celem jest przetwarzanie i zapisywanie danych. Razem z pamięcią komputera i twardym dyskiem tworzy podstawową część komputera.

Profil użytkownika: zestaw informacji opisujący użytkownika oprogramowania, strony internetowej bądź innego rodzaju narzędzia komputerowego. Obejmuje on zazwyczaj informacje takie jak nazwa użytkownika, hasło oraz pozostałe dane personalne (np. data urodzenia, zainteresowania).

Profil: w portalach społecznościowych, komunikatorach, czatach i grach internetowych profilem określa się informacje na temat użytkownika. Profile tworzone są przez użytkowników sieci i mogą być one prywatne bądź dostępne dla innych osób.

Program antyspyware, program antywirusowy: to programy, które zwalczają spyware lub wirusy. Programy takie skanują wszystkie pobierane z Internetu pliki, a następnie blokują te, które mogą być niebezpieczne dla komputera i jego użytkowników.

Program komputerowy (oprogramowanie, software): składa się z uporządkowanej sekwencji instrukcji pozwalających na korzystanie z komputera, które napisane zostały przez programistów komputerowych. Oprogramowanie, które kupujemy, zapisywane jest najczęściej na płytach CD lub DVD.

Oprogramowanie próbne (testowe): oprogramowanie, które można wypróbować zanim postanowimy je kupić. Próbne wersje zazwyczaj nie różnią się od pełnych wersji oprogramowania, można z nich jednak korzystać jedynie przez określony czas np. 30 dni, lub określoną ilość razy np. 10 uruchomień.

Prywatność: zdolność osoby lub grupy do kontrolowania przepływu informacji na ich własny temat, jednocześnie pozwalająca na częściowe ujawnienie informacji o sobie. Prywatność jest czasami łączona z anonimowością, czyli pragnieniem pozostania niezauważonym przez innych.

Prywatne dane: wszelkie informacje dotyczące pojedynczych osób lub całych grup, które nie powinny zostać upublicznione. Kiedy coś jest dla jednej osoby sprawą prywatną, zazwyczaj traktujemy to jako coś specjalnego i jesteśmy na tym punkcie bardzo wrażliwi.

Przeglądanie (surfowanie): czynność polegająca na korzystaniu z przeglądarki internetowej w celu oglądania stron internetowych.

Przeglądarka: program komputerowy wykorzystywany do oglądania stron internetowych. Do najbardziej popularnych przeglądarek intenetowych należą Mozilla Firefox, Opera, Internet Explorer, Safari. Najnowsze wersje przeglądarek zawierają zaawansowane funkcje kontroli rodzicielskiej.

Przemoc w sieci: odnosi się do stosowania przemocy w mediach elektronicznych, najczęściej w komunikatorach, czatach i e-mailach. Poprzez przemoc w sieci rozumieć należy powtarzające się akty przemocy, gróźby, wygłaszanie uwag na tle seksualnym oraz wygłaszanie negatywnych komentarzy na temat danej osoby. Osoby znęcające się nad innymi często publikują dane kontaktowe do osób, które prześladują, a

niekiedy nawet przybierają ich tożsamość, ośmieszając lub zniesławiając swoje ofiary.

Raportowanie: funkcja pozwalająca użytkownikom sieci na zgłaszanie moderatorowi lub webmasterowi różnego rodzaju problemów (m.in. technicznych, o nieprawidłowym zachowaniu innych użytkowników strony), związanych z działaniem stron WWW.

Robak (worm): specjalny rodzaj wirusa, który rozprzestrzenia się przez Internet. Jego celem jest zniszczenie naszych dokumentów, zamykanie komputera czy też spowalnianie szybkości przesyłu danych przez Internet.

Second Life: znana trójwymiarowa wspólnota internetowa. Użytkownicy mogą komunikować się z innymi użytkownikami sieci za pomocą awatara (zobacz definicję), budować domy, zmieniać środowisko w którym żyją, zajmować się wirtualnym handlem i zarabiać wirtualne pieniądze.

Sieć WWW: skrót od angielskiego słowa World Wide Web. Jest to zestaw plików i dokumentów internetowych sformatowanych w formacie HTML, zawierających linki do innych plików i dokumentów takich jak np. grafika, pliki audio czy wideo. Sieć WWW jest częścią Internetu.

SIP-Bench: raport powstały przy współudziale Komisji Europejskiej, mający na celu zbadanie efektywności 30 narzędzi antyspamowych pod względem ochrony dzieci przed szkodliwymi treściami, jakie znaleźć można w Internecie.

Skanowanie: procesy zamiany tekstu drukowanego na cyfrowy przy wykorzystaniu skanera. Zamiana ta pozwala na przeglądanie dokumentów elektronicznych na komputerze i przesyłanie ich dalej drogą internetową.

Social networking (sieć społeczna): polega na pielęgnowaniu i powiększaniu ilości naszych znajomych w sieci poprzez udział w społecznościach internetowych, których członkowie mają podobne zainteresowania. Członkowie danej wspólnoty kontaktują się ze sobą w sieci za pomocą odpowiedniego oprogramowania, które należy zainstalować na komputerze (zobacz portale społecznościowe).

Spam: niechciane wiadomości e-mail, zazwyczaj o charakterze handlowym, które wysyłane są w dużych ilościach. Spamowanie to jedno z najczęstszych nadużyć stosowanych w Internecie.

Spyware: złośliwe oprogramowanie, które załączone jest do plików pobranych z sieci. Spyware instaluje się samoczynnie i monitoruje wszystko to, co robimy na komputerze, a następnie wysyła informacje na ten temat do innych osób. Są to zazwyczaj różnego rodzaju firmy zainteresowane poznaniem profili użytkowników sieci w celu wysyłania im reklam lub innych informacji. Informacje tego rodzaju są też często wysyłane do crackerów, którzy chcą mieć dostęp do naszych prywatnych plików i danych.

Strona główna: strona internetowa, która pojawia się automatycznie, kiedy uruchomimy przeglądarkę internetową. Termin ten jest także stosowany do określania strony głównej danej strony internetowej (zobacz definicja).

Strona internetowa (witryna WWW, website): dokument pobierany z Internetu i wyświetlany na komputerze za pomocą przeglądarki, utworzony najczęściej w języku HTML lub PHP. Strony internetowe zazwyczaj zawierają linki do innych stron i plików multumedialnych umieszczonych w sieci. Zbiór takich dokumentów umieszczony pod jednym adresem WWW tworzy witrynę internetową, której właścicielem może być osoba prywatna, organizacja bądź firma. Zarządzaniem witryną internetową zajmuje się webmaster.

Subskrybowanie: dobrowolne zapisanie się w celu korzystania z danej usługi lub w celu otrzymywania aktualnych informacji, które będą wysyłane na naszą skrzynkę e-mail. Użytkownicy powinni mieć możliwość zrezygnowania z danej usługi w dowolnym momencie. Często wymaga podania danych osobowych.

System operacyjny: program, który obsługuje podstawowe funkcje komputera, dzięki któremu na naszym komputerze może działać pozostałe oprogramowanie. Przykładami systemów operacyjnych są Mac OS X, Linuks i Windows.

Szkodliwe treści: zdjęcia, teksty, dokumenty, których treść może być szkodliwa. Przykładem szkodliwych treści mogą być zdjęcia przedstawiające przemoc.

Tapeta: wzór, zdjęcie bądź innego rodzaju obraz graficzny, który umieścić można na monitorze komputera.

Transfer pliku: proces wysyłania pliku z jednego komputera na drugi. Z punktu widzenia użytkownika sieci proces ten utożsamiany jest z pobieraniem plików z sieci (ang. downloading) oraz umieszczaniem plików w sieci (ang. uploading).

Ulubione (Zakładki): folder utworzony przez użytkownika sieci, w którym można zapisać ciekawe linki do stron internetowych. Mogą być one podzielone na foldery, w nazwie których zostaną zawarte słowa kluczowe ułatwiające znalezienie poszukiwanej strony WWW.

URL: adres strony internetowej lub pliku w sieci. Korzysta z symbolu / (ukośnik) w celu określenia lokalizacji różnych katalogów. Pierwsza część adresu określa rodzaj wykorzystywanego protokołu internetowego - http://, druga natomiast zawiera nazwę domeny,na której dany dokument/ strona internetowa zostały zlokalizowane - www.google.pl.

Ustawienia bezpieczeństwa (profilu): opcje bezpieczeństwa związane z naszym profilem w Internecie (zobacz definicję). Zazwyczaj opcje odnoszą się do otwierania zdjęć i plików oraz określenia bezpiecznych źródeł otrzymywania danych. Ustawienia bezpieczeństwa stosowane są w przypadku dostępu do treści przeznaczonych dla dorosłych.

Ustawienia prywatności: zestaw ustawień stopnia prywatności naszego konta, które można edytować w celu zwiększenia poziomu naszej prywatności. Celem jest nie ujawnianie danych osobowych, cookies, itd.

Ustawienia rodzinne (kontrola rodzicielska): ustawienia przeglądarki i innych narzędzi internetowych, mające na celu m.in. filtrowanie treści oglądanych przez dzieci, ograniczanie ilości czasu, jaki dzieci mogą spędzać przed komputerem.

VoIP (Voice over IP): pozwala użytkownikom Internetu na prowadzenie rozmów w sieci. Możliwe jest to po zainstalowaniu odpowiedniego oprogramowania. Rozmowy między użytkownikami korzystającymi z tego samego oprogramowania VoIP mogą być bezpłatne (np. Skype, GoogleTalk). Oprogramowanie to pozwala także na wymianę plików i prowadzenie czatów.

Wirus: rodzaj szkodliwego kodu bądź złośliwego oprogramowania, które działa na komputerze. Zazwyczaj wirusy są w załącznikach do e-maili, możliwe jest także zakażenie komputera poprzez przenośne nośniki pamięci (pendrive'y, płyty CD).

Własność wirtualna: zestaw rzeczy, których właścicielem jest każdy z uczestników biorących udział w grze internetowej. Każdy gracz posiada swoją własność wirtualną, którą można zobaczyć jedynie na ekranie monitora.

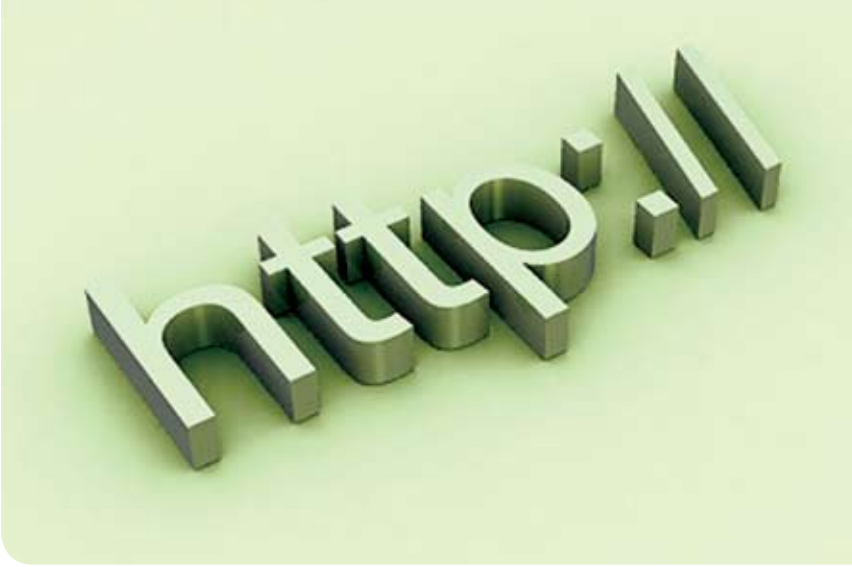
Wymiana plików: wysyłanie plików do innych użytkowników sieci (ang. uploading) oraz pobieranie plików z Internetu (ang. downloading). Zazwyczaj wymiana plików jest możliwa dzięki programom typu P2P (ang.peer-to-peer).

Wyskakujące okienko (popup): okienko, które nagle pojawia się, jeżeli wchodzimy na stronę internetową

lub korzystamy z klawiszy funkcyjnych. Wyskakujące okienka zazwyczaj posiadają listę poleceń i pozostają na ekranie dopóki nie wybierzemy jednej z opcji lub do chwili, gdy klikając prawym klawiszem myszy w krzyżyk w prawym górnym rogu nie zamkniemy wyskakującego okienka.

Wyszukiwarka: strona przeznaczona do poszukiwania informacji na stronach internetowych. Najbardziej popularną wyszukiwarką jest Google. Wyszukiwarki posiadają zaawansowane opcje dotyczące bezpieczeństwa korzystania ze stron WWW.

Załącznik: to plik, który wysyłany jest razem z e-mailem. Często w załącznikach znaleźć można wirusy i robaki. Należy być szczególnie ostrożnym w sytuacji, gdy otrzymujemy od nieznajomej osoby e-mail z załącznikiem.



E. E. Przydatne linki do stron internetowych

AWARENESS - INSAFE

strona projektu „Awareness", prowadzona przez organizację INSAFE:
http://www.saferinternet.org

PROGRAM KOMISJI EUROPEJSKIEJ SAFER INTERNET PLUS

Strona projektu Safer Internet w Polsce:
http://www.saferinternet.pl

NIFC HOTLINE POLSKA

Punkt kontaktowy ds. zwalczania nielegalnych treści w Internecie:
http:/www.dyzurnet.pl

DZIEŃ BEZPIECZNEGO INTERNETU

strona Dnia Bezpiecznego Internetu:
http://www.dbi.pl

OGÓLNOPOLSKA KAMPANIA NA RZECZ BEZPIECZEŃSTWA DZIECI W INTERNECIE

strona kampanii społecznej "Dziecko w Sieci":
http://www.dzieckowsieci.pl

POMOC W SYTUACJACH ZAGROŻENIA BEZPIECZEŃSTWA DZIECI I MŁODZIEŻY W INTERNECIE

Pomoc dla dzieci i ich opiekunów w sytuacji, gdy coś złego przydarzy się w Internecie:
http://www.helpline.org.pl

OSWAJANIE SIECI

Serwis edukacyjny dla dzieci i rodziców na temat bezpieczeństwa w Internecie:
http://www.upclive.pl/dzieci

SIECIAKI

Serwis edukacyjny dla dzieci:
http://www.sieciaki.pl

PRZEDSZKOLAKI SIECIAKI

Edukacyjny serwis dla najmłodszych użytkowników Internetu:
http://www.przedszkolaki.sieciaki.pl

DZIECI NICZYJE

Strona Fundacji "Dzieci Niczyje":
http://www.fdn.pl

NASK

Naukowa i Akademicka Sieć Komputerowa:
http://www.nask.pl

ins@fe

Partnerem jest: upc

Tytuł: Bezpieczeństwo w Internecie - przewodnik dla całej rodziny • Napisany przez Insafe/Liberty Global / UPC w 2008 roku
Prefiks: 9789078209 • Id 51950 • Numer ISBN: 9789078209577 • EAN : 9789078209577