**Szkodliwe kontakty**– zdarzyć się może, że ktoś obrazi Cię na czacie, wyśle nieprzyjemnego e-maila lub wiadomość na komunikatorze, a może po prostu pisze do Ciebie, choć Ty tego nie chcesz. Może to być ktoś, kto Cię zna, ale może też to być osoba nieznajoma, która uważa, że takie zachowanie to dobry żart. Zwykle ktoś taki myśli też, że w Internecie można robić, co się chce i nikt nie dowie się, kim jest. To nieprawda. W Internecie każdy zostawia ślady, po których policja może go znaleźć. Jeśli zdarzy Ci się, że internetowy kontakt sprawia Ci przykrość, powiedz o tym rodzicom lub zaufanej osobie dorosłej. Możesz również skontaktować się z helpline.org.pl.  
  
**Ujawnienie Twoich prywatnych danych**– Twoje prywatne dane nie powinny wpaść w niepowołane ręce! Adres e-mail, numer telefonu, adres, zdjęcie czy różnego rodzaju hasła (do poczty, komunikatora, czatu) to informacje, które należy chronić w trosce o własne bezpieczeństwo. Przecież nie chcesz dostawać spamu lub żeby każdy wiedział, gdzie mieszkasz i mógł do Ciebie przyjść czy zmienił tak Twoje zdjęcie w komputerze, że będzie Ci przykro, będą się z Ciebie śmiać. To samo dotyczy danych Twoich kolegów i koleżanek – odmawiaj, jeśli ktoś Cię o to poprosi – nie chcesz, by im stało się coś złego.  
  
**Szkodliwe treści**– to takie teksty, zdjęcia, filmy i nagrania, które są nielegalne lub przeznaczone tylko dla dorosłych. Kontakt z nimi może być dla Ciebie przykry, mogą Cię przestraszyć, zawstydzić lub spowodować, że poczujesz się źle. Pamiętaj, że możesz na nie natrafić zupełnie przypadkowo, to się zdarza i nie ma w tym Twojej winy. Jeśli zdarzyło Ci się napotkać w Internecie szkodliwe treści – powiedz o tym rodzicom lub zaufanej osobie dorosłej, a ona niech skontaktuje się z dyżurnet.pl, aby treści te zostały usunięte i nikomu już nie zagrażały.  
  
**Wirusy i złośliwe programy**– wirusy i inne złośliwe programy mogą zniszczyć pliki na Twoim komputerze, albo sprawić, że korzystanie z niego będzie trudne lub nawet niemożliwe – przestanie działać tak, jak powinien. Nie ma całkowicie skutecznej ochrony przed wirusami i złośliwymi programami. Chronić należy się poprzez stosowanie antywirusa (pamiętaj o regularnym uaktualnianiu jego bazy – pozwoli mu to rozpoznawać nowe zagrożenia) i zapory sieciowej. Bardzo ważne jest również korzystanie tylko z tych programów, płyt, dyskietek i pendrive’ów, na których wiemy co się znajduje. Tę samą zasadę warto stosować również do nieznanych stron internetowych.  
  
**Spam** – spam można porównać do ulotek zostawianych przed drzwiami lub wkładanych za wycieraczki samochodów. To wiadomości e-mail, które trafiają na Twoją skrzynkę, choć nie czekałeś na nie i nie są Ci potrzebne. Spam może przeszkadzać w znalezieniu w nim listu na który czekasz, może też zawierać szkodliwe treści i wirusy. Dlatego warto korzystać w anty-spamu w poczcie, a swój adres e-mail chronić i nie podawać nikomu bez potrzeby, zwłaszcza w Internecie, gdzie każdy może go znaleźć.  
   
**Włamania** – zdarzyć się może, że ktoś zobaczy, jakie hasło wpisujesz logując się na pocztę, do komunikatora czy na czacie. Może się też zdarzyć, że hasło jest bardzo proste i może je zgadnąć każdy, kto będzie miał trochę szczęścia lub dobrze Cię zna. Znając Twoje hasło, osoba taka może zrobić co tylko chce, a dla innych użytkowników Internetu wyglądać to będzie na Twoje działania. Aby uniknąć kłopotów i nieprzyjemności wymyślaj dobre hasła, to jest długie i skomplikowane. Nie używaj jako haseł imienia swojego, przyjaciela, czy zwierzaka, daty urodzenia itd. – te hasła są popularne i łatwo je odgadnąć