

Dzień obchodzony w połowie lutego od 2005 roku, ustanowiony z inicjatywy Komisji Europejskiej. Ma na celu kształtowanie świadomości społecznej dotyczącej niebezpieczeństw, na które narażone są osoby korzystające z Internetu – zwłaszcza dzieci i młodzież. Anonimowość w sieci o powszechny dostęp do cyberprzestrzeni niosą ze sobą całą gamę zagrożeń. Do najczęściej występujących należą uwodzenie dzieci przez dorosłych o skłonnościach pedofilskich, pornografia oraz cyberprzemoc, czyli publikacja obraźliwych lub kompromitujących materiałów dotyczących innych osób. Wielka odpowiedzialność spoczywa w tych kwestiach na rodzicach, których zadaniem jest przygotowanie dzieci do właściwego korzystania z sieci. Dlatego też zarówno szkoły, jak i organizacje pozarządowe zachęcane są do organizowania szkoleń i projektów mających na celu zwiększenie bezpieczeństwa w Internecie. Wirtualny świat to jednak nie tylko zagrożenia dla dzieci, ale również dla wszystkich uczestników cyberprzestrzeni. Codziennie powstaje grubo ponad 100 tysięcy nowych wirusów. Niektóre z nich to zwykła złośliwość hakerów, inne z kolei mają na celu kradzież cennych informacji, takich jak numery kont czy numery pin. Dotyczy to już nie tylko komputerów, ale również smartfonów i tabletów. Wśród aplikacji najbardziej podatnych na ataki złośliwego oprogramowania znajdują się tak popularne nazwy jak Java, Acrobat Reader czy Adobe Flash. Warto zatem każdego dnia w roku korzystać z dobrego programu antywirusowego.

Przydatne strony:

www.dzieckowsieci.pl

www.sieciaki.pl

www.brpd.gov.pl

www.dyzurnet.pl

www.pegi.info

www.saferinternet.pl

POMOC

Bezpłatny numer telefonu: **0 800 100 100**

Jak bezpiecznie korzystać z Internetu?

Gdy chodzi o bezpieczeństwo, najważniejszy jest prosty przekaz, dlatego też zebraliśmy najważniejsze wskazówki dotyczące bezpiecznego korzystania z Internetu, które są następujące:

- zawsze korzystaj z aktualnego systemu operacyjnego, aktualnej przeglądarki internetowej i aktualnego programu antywirusowego,
- twórz bezpieczne hasła logowania do poczty e-mail i kont w rozmaitych usługach – nie zawieraj w nich oczywistych słów oraz informacji takich jak imię czy data urodzenia i staraj się wymyślać długie hasła,

- nie korzystaj z tego samego hasła na różnych stronach,
- nie loguj się do ważnych usług, korzystając z publicznych hotspotów Wi-Fi (bo one szczególnie są narażone na cyberwłamania),
- podczas logowania dwa razy sprawdź adres WWW strony i upewnij się, że strona logowania ma certyfikat bezpieczeństwa (warto też – jeśli to możliwe – korzystać z weryfikacji dwuetapowej),
- nie podawaj w Internecie żadnych danych i nie udostępniaj żadnych zdjęć, do których dostępu nie powinny uzyskać żadne „strony trzecie”,
- nie wchodź na strony z linków w podejrzanych wiadomościach e-mail i nie otwieraj dodanych do nich załączników
- uważaj na skrócone adresy URL, które często mogą stanowić pułapkę.

„Wielu internautów ignoruje kwestię bezpieczeństwa swojej cyfrowej tożsamości, ponieważ nie zdają sobie sprawy z zagrożeń lub nie uważają siebie samych za interesujący dla cyberprzestępców cel ataku. W ten sposób przeprowadzenie ataku staje się niezwykle łatwe.