

Zasady bezpiecznego korzystania z Internetu

Rozwój technologii informatycznych wiąże się z popularyzacją komunikacji z ludźmi zupełnie anonimowymi. Coraz częściej korzystamy z różnego typu ułatwień, które niesie Internet, czy to kontakt ze znajomymi, czy zakupy na odległość, czy też zamówienie biletów do kina. Jednakże korzystanie z Internetu wiąże się też z różnymi niebezpieczeństwami. Ważnym aspektem zabezpieczenia się przed cyberprzestępstwami jest z pewnością korzystanie z odpowiednich programów antywirusowych, antyspyware (zabezpieczają przed programami szpiegującymi), firewall (ochrona przed atakami hakerów oraz złośliwym oprogramowaniem). Należy pamiętać, aby programy te pochodziły z legalnego źródła i były uaktualniane. Program antywirusowy jest dobry do momentu, gdy ma aktualną bazę sygnatur wirusów. Ważnym aspektem ochrony jest również aktualizacja systemu operacyjnego, a także przeglądarek oraz dodatków (java, flash). To tu najczęściej pojawiają się luki, które umożliwiają dostęp do komputera przez osoby nieuprawnione. Warto pamiętać o następujących zasadach korzystania z Internetu.

1. Ceniśmy prywatność.

Pamiętaj o chronieniu prywatności swojej oraz swojej rodziny, znajomych. Zwracaj uwagę komu i gdzie podajesz dane osobowe, wysyłasz swoje zdjęcia. Nic co trafia do Internetu, nie ginie!

2. Wybierajmy zaufane portale.

Szukając ofert należy korzystać ze znanych i zaufanych portali. Sprawdzajmy również opinie innych internautów na temat danej firmy. Warto zauważyć, że bezpieczniejsze jest korzystanie ze specjalistycznych portali transakcyjnych. Jeżeli za pośrednictwem takiego portalu popełnione zostanie oszustwo, mamy większe szanse na wyjaśnienie

sprawy przez policję. Mianowicie, spółka prowadząca portal posiada wiele niezbędnych informacji, które z pewnością ułatwią policji prowadzenie dochodzenia. Zauważyć należy, że również sama spółka może wywierać nacisk na nieuczciwego użytkownika. Wszystkie te aspekty zwiększają bezpieczeństwo transakcji.

3. Stosujmy trudne hasła.

Stosowanie haseł typu „kasia1999” z pewnością jest łatwe do zapamiętania, ale jednocześnie łatwe do złamania. Aby hasło było silne należy stosować zarówno litery, cyfry, a także znaki specjalne, np. #, _, &. Użycie klawisza shift ze znakami z poprzedniego hasła umacnia je i w efekcie otrzymujemy hasło: „kAsi@!99(”. Warto jednak starać się, aby nasze hasło nie stanowiło oczywistych ciągów znaków, np. będących imieniem, datą urodzenia, popularnych słów.

4. Różne konta, różne hasła.

Korzystajmy z różnych haseł do różnych kont. Warto również posiadać różne konta mailowe do różnych celów (np. zawodowych, społecznościowych itp.).

5. Uwaga rejestracja!

Rejestracja oraz instalacja oprogramowania to ważny proces. Zatem przeczytajmy dokładnie informacje, które nam są przekazywane. Sprawdźmy, czy rzeczywiście na musimy się na wszystko zgodzić (takie pola najczęściej zaznaczane są symbolem *).

6. Masz e-mail!

Nie otwieraj podejrzanych wiadomości e-mail, a w żadnym wypadku nie wysyłaj swoich haseł dostępu.

7. Praca na cudzym komputerze.

Używając ogólnodostępnych komputerów korzystaj z przeglądarki w trybie incognito.

8. Rozsądnie pobieraj.

Dane pobieraj tylko z zaufanych i zweryfikowanych witryn oferujących legalne oprogramowanie.

9. Hotspot nie do wszystkiego.

Korzystając z Hotspotów oraz innych ogólnodostępnych sieci lepiej zrezygnować z logowania się do konta bankowego oraz innych ważnych kont.

10. Bankujesz? Zachowaj ostrożność.

Korzystając ze stron bankowych, sprawdzajmy, czy nawiązane zostało połączenie szyfrowane. Świadczy o tym początek adresu *https://* oraz symbol zamkniętej kłódki. Dodatkowo można sprawdzić informacje o certyfikacie cyfrowym, m. in. jego ważność, na kogo jest wystawiony. W tym celu należy kliknąć na symbol kłódki i zapoznać się z informacjami.