BEZPIECZNY INTERNET w pracy zdalnej i na co dzień

1. Zainstaluj na komputerze oraz uruchom:
   a) Oprogramowanie antywirusowe.
   b) Zaporę ogniową z systemem ochrony przed włamaniami.

2. Regularnie, jak tylko jest dostępna, przeprowadź aktualizację oprogramowania zainstalowanego na komputerze, a zwłaszcza systemu operacyjnego, przeglądarki internetowej i innych aplikacji, które korzystają z Internetu.

3. Jak najczęściej aktualizuj, bazy sygnatur oprogramowania antywirusowego.

4. Aktualizując oprogramowanie zawsze korzystaj z zaufanych stron internetowych, najlepiej producenta danego pakietu oprogramowania.

5. Ważne aby podczas korzystania z przeglądarki upewniać się, że adres wpisany w pasku adresu jest poprawny. Łatwo jest się pomylić. Złodzieje internetowi bardzo często wykorzystują literówki w adresach stron internetowych, aby wyłudzić od ciebie dane osobowe lub cię okraść.

6. Domyślnie w Internecie (ze szczególnym uwzględnieniem poczty elektronicznej) informacje są przesyłane w jawnej postaci (nie są szyfrowane). Mogą być one przechwycone i odczytane przez osoby nieupoważnione. Dlatego, aby zapewnić poufność lub integralność przesyłanych danych, jeśli jest to tylko możliwe, to korzystaj z połączeń szyfrowanych z wykorzystaniem protokołu TLS/SSL. Potwierdzeniem nawiązania bezpiecznego połączenia jest ikona kłódki umieszczana (w zależności od przeglądarki internetowej) obok paska URL lub w dolnej części ekranu przeglądarki, a także adres URL rozpoczynający się od „https”.

7. Nie odpowiadaj na wiadomości pocztowe, w których jesteś proszony(a) o podanie lub zweryfikowanie poufnych wiadomości (np. danych osobowych, identyfikatorów i haseł dostępu, numer konta lub karty kredytowej itp.).

8. Unikaj klikania na podejrzane linki podawane w wiadomościach pocztowych lub na stronach WWW.

9. Nie otwieraj, nie uruchamiaj i nie instaluj żadnych plików lub programów (w szczególności z rozszerzeniem „exe”, „com”, „bat”, „reg”, „scr”, „cpl”, „vbs”, „js”, „pif”, „jar”) nieznanego pochodzenia, pobranego z niezaufanej strony WWW lub otrzymanego pocztą elektroniczną. Jeżeli wiadomość pochodzi od znanego nadawcy, przed otwarciem zaleca się sprawdzić załącznik za pomocą programu antywirusowego i ewentualnie potwierdzić, że taka wiadomość została wysłana przez nadawcę.

10. Zachowaj szczególną ostrożność podczas otwierania wiadomości pocztowych pochodzących od nieznanych nadawców.

11. Zachowaj szczególną ostrożność podczas korzystania z Internetu w miejscach publicznych lub za pomocą łączy radiowych (np. w kafejkach internetowych, hot spot, itp.). Ogranicz w takim przypadku do minimum wykonywanie zakupów w sklepach internetowych lub dostęp do usług bankowości elektronicznej