

Zasady bezpiecznego korzystania z poczty elektronicznej

Nie zapisuj hasła do swojej poczty w przeglądarce

Traktuj pocztę elektroniczną jak system bankowy. Nigdy nie zapisuj hasła do swojej poczty w przeglądarce internetowej. Uchroni Cię to przed dostępem do niej przez osoby niepowołane lub wykradzeniem hasła przez wirusy bezpośrednio z systemu przeglądarki.

Zawsze pamiętaj by się wylogować

Wyrób w sobie nawyk wylogowania się z poczty elektronicznej. Wiele systemów w szczególności on-line, posiada ustawioną bardzo długą sesję. To znaczy, że jeśli się raz zalogujesz, pozostajesz zalogowany przez wiele dni. Jest to bardzo niebezpieczne.

Używaj silnego i unikalnego hasła do skrzynki pocztowej

Cyberprzestępcy mają dostęp do milionów jak nie miliardów standardowych haseł. Używając prostych haseł umożliwiasz im włamanie się na Twoje konto z użyciem metod Brute Force. W hasłach nie używaj imion czy nazwisk swoich lub osób najbliższych. Nie używaj numerów identyfikacyjnych np. PESEL czy dat urodzenia. Hasło powinno być długie, zawierać znaki specjalne, spacje i raczej być w formie zdania niż pojedynczego sformułowania. Do wrażliwych serwisów jak skrzynki pocztowe stosuj różne, unikalne hasła. Złamanie hasła w innych serwisach w których masz konta nie spowoduje automatycznie przechwycenia kolejnych kont usługowych.

Nigdy nie udostępniaj swojego hasła

Nigdy nie udostępniaj swojego hasła do kont pocztowych żadnym osobom trzecim. Jest to bardzo niebezpieczne a co więcej nie będziesz miał żadnej informacji o tym, co ta osoba przeglądała w twojej poczcie.

Zawsze weryfikuj nadawcę

Zawsze sprawdzaj nadawcę wiadomości oraz domenę z której jest ona przysłana. Wprawny haker co prawda jest w stanie podszyć się pod dowolny adres ale coraz większa ilość usługodawców pocztowych jest w stanie wykrywać takie wiadomości i je blokować. Nie mniej jednak, cyberprzestępcy wysyłając fałszywe wiadomości stosują adresy mailowe o podobnej nazwie do banków czy dużych usługodawców, co może uśpić Twoją uwagę. Weryfikując nadawcę sprawdzaj adres e-mail z jakiego przyszła wiadomość a nie nazwę.

Sprawdź poprawność pisowni wiadomości

Wiele wiadomości wysyłanych jest automatycznie przez roboty. Często wiadomości te są automatycznie tłumaczone z innych języków. Sprawia to, że treść wiadomości posiada głównie błędy stylistyczne i gramatyczne. Jeżeli otrzymasz wiadomość z łamaną polszczyzną, możesz być niemal pewien że było ona wygenerowana z translatora. Bądź ostrożny przy takich wiadomościach.

Nie odpowiadaj na SPAM

Odpowiadanie na SPAM potwierdza istnienie adresu e-mail a tym samym może wygenerować kolejną dawkę niechcianych wiadomości.

Nie klikaj w linki umieszczone w mailach

Nigdy nie klikaj w linki zamieszczone w mailach. Jeżeli wiadomości mają postać HTML, możesz zostać przekierowany na inną stronę niż podana w treści wiadomości. Lepiej wkleić link do paska adresu w przeglądarce i przed uruchomieniem sprawdzić jaką ma postać. Linkowanie do dziwnej nieznanej strony powinno stanowić dla Ciebie ostrzeżenie.

Uważaj na podejrzane załączniki nawet od znajomych

Hakerzy często wysyłają SPAM i wirusy z przejętych kont do listy kontaktów. Otrzymując wiadomość od rodziny, znajomych lub znanych kontrahentów Twoja czujność jest uśpiona. Uważaj w szczególności na pliki spakowane ZIP, RAR, 7-ZIP itp. oraz dokumenty PDF, które bardzo często transportują wirusy.

Nie wysyłaj wrażliwych danych bez szyfrowania

Nigdy nie wysyłaj wrażliwych danych pocztą elektroniczną w formie niezabezpieczonej. Wrażliwe są wszelkie informacje, numer PESEL, wiek, miejsce zamieszkania, skany dokumentów itp. Jeżeli musisz przekazać takie dokumenty lub informacje, wprowadź je w oddzielnym dokumencie, spakuj do archiwum zip, rar, 7z lub innego z hasłem, a następnie prześlij zaszyfrowane. Hasło zawsze dostarczaj innym kanałem np. poprzez SMS lub komunikator.