

## ZASADY BEZPIECZNEGO KORZYSTANIA Z POCZTY MAILOWEJ

- 1) w sprawach służbowych do korespondencji mailowej używaj wyłącznie służbowego adresu mailowego przydzielonego Tobie w naszej szkole;
- 2) nie prowadź korespondencji mailowej przy użyciu prywatnego adresu mailowego, a gdyby użycie prywatnej poczty było niezbędne do wykonywanych przez Ciebie obowiązków, uprzedź o takim działaniu dyrektora szkoły i upewnij się, że takie działanie jest przez niego akceptowane;
- 3) nie wykorzystuj służbowej poczty mailowej do celów prywatnych;
- 4) zanim otworzysz nadesłany mail, ustal czy:
  - znasz nadawcę wiadomości,
  - otrzymałeś już inne wiadomości od tego nadawcy,
  - spodziewasz się otrzymać taką wiadomość,
  - tytuł wiadomości i nazwa załącznika mają sens,
  - wiadomość nie zawiera złośliwego oprogramowania i jaki jest wynik skanowania antywirusowego,po tych ustaleniach podejmij decyzję, czy dopuszczalne jest otworenie wiadomości, załączników, linków, jeśli wiadomość budzi Twój niepokój, skonsultuj się z inspektorem ochrony danych;
- 5) bardzo uważnie prowadź korespondencję mailową - uważaj na ataki phishingowe, fałszywe maile, linki aktywujące złośliwe oprogramowanie;
- 6) pamiętaj, że złośliwe oprogramowanie, bywa przesyłane w postaci załączników do maili lub pobierane jest po kliknięciu w odnośnik zawarty w mailu, dlatego nie otwieraj załączników (plików) w korespondencji mailowej nadesłanej przez nieznanego nadawcę lub załączników, których nie oczekiwałeś, które nie mają związku z treścią maila, które budzą Twoją nieufność - jeśli chcesz zweryfikować prawidłowość korespondencji, zrób to poprzez kontakt z nadawcą innym kanałem komunikacji (kontakt telefoniczny, za pośrednictwem dziennika elektronicznego, itp.), każdy podejrzany e-mail zgłaszaj do inspektora ochrony danych;
- 7) każdy załącznik w poczcie traktuj jako "niebezpieczny" - przed otwarciem zapisz go na dysku, zweryfikuj typ pliku i sprawdź programem antywirusowym - pamiętaj, że nawet "bezpieczne" pliki (DOC, PDF) mogą zawierać wirusy;
- 8) zwracaj uwagę dokąd prowadzą odnośniki (linki) do stron internetowych zamieszczone w poczcie - fałszywe zwykle są długie lub zawierają literówki (np. "wydzialoswiatyjsf" zamiast "wydzialoswiatyjt"), absolutnie nie klikaj w takie odnośniki;
- 9) pamiętaj, że *phishing* to rodzaj oszustwa, w której przestępca żeruje na naiwności osoby, z którą się kontaktuje, jej słabościach, współczuciu, chęci pomocy, często polega na podszywaniu się pod inną osobę lub instytucję w celu wyłudzenia informacji (np. danych logowania, innych

danych dostępowych do systemów informatycznych, danych osobowych, informacji poufnych) czy zainfekowania urządzenia szkodliwym oprogramowaniem, a także skłonienia ofiary do pewnych działań, z reguły dla niej niekorzystnych, dlatego bardzo uważnie czytaj nadsyłane komunikaty, analizuj adresy mailowe - ustal, czy są rzeczywiste, czy tylko łudząco podobne do adresów, z którymi masz zazwyczaj do czynienia (np. adresów urzędów, urzędników obsługujących naszą placówkę, banków, centrów usług wspólnych, rady rodziców, itp.);

- 10) uważaj na spam, a więc niezamawiane wiadomości - najlepiej kasuj je trwale niezwłocznie po otrzymaniu;
- 11) jeśli w korespondencji mailowej przesyłasz dane osobowe upewnij się, że:
  - nie przesyłasz ich w nadmiernym zakresie (często wystarczy imię i nazwisko bez nr PESEL czy daty urodzenia),
  - prawidłowo określasz krąg adresatów (nie ufaj autouzupełnianiu - zawsze sprawdź do kogo kierujesz wiadomość),
  - załączniki są właściwie zabezpieczona poprzez mechanizmy kryptograficzne (pakowanie i hasłowanie wysyłanych plików, podpis elektroniczny, itp),
  - unikaj używania danych osobowych lub poufnych informacji w temacie wiadomości,
- 12) przed wysłaniem maila upewnij się, że wysyłasz go do właściwego adresata - zwróć uwagę na poprawność adresu odbiorcy;
- 13) unikaj korespondencji seryjnej, a jeśli ją stosujesz upewnij się, że wszyscy adresaci rzeczywiście mają otrzymać wysłaną wiadomość i zastosuj opcję "ukryte do wiadomości";
- 14) nie przesyłaj w tym samym mailu informacji zaszyfrowanej razem z hasłem (hasło najlepiej przekazać innym kanałem komunikacji);
- 15) poproś adresata o potwierdzenie otrzymania maila i zapoznania się z informacją, a jeżeli jest to technicznie możliwe, skorzystaj z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu;
- 16) przestrzegaj zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych;
- 17) nie rozsyłaj za pośrednictwem poczty informacji niezwiązanych z wykonywanymi zadaniami w szkole, w tym zdjęć, filmików, żartów, "łańcuszków szczęścia" itp.;
- 18) nie rozsyłaj wiadomości zawierających załączniki o dużym rozmiarze do większej liczby adresatów, jeśli masz potrzebę wysłać załącznik o dużym rozmiarze (np. film), w celu ustalenia sposobu dokonania przesyłki, skontaktuj się z inspektorem ochrony danych;
- 19) w miarę możliwości i zgodnie z zasadami archiwizowania okresowo kasuj zbędne maile.