

Podstawowe zasady bezpiecznego przeglądania korespondencji elektronicznej

1. Należy upewnić się czy nadawca jest nam znany oraz czy faktycznie oczekiwaliśmy takiej korespondencji.
2. Nie należy otwierać korespondencji w sposób oczywisty nie związanej z pełnionymi obowiązkami. Jeśli otrzymujemy fakturę w Wydziale nie obsługującym w żaden sposób płatności, to nie otwieramy takiego maila.
3. Należy zwracać uwagę na otwierane załączniki. Złośliwe oprogramowanie może być ukryte pod dowolnym plikiem, także multimedialnym, np. pliki graficzne, PDFy, MS Word lub MS Excel, wideo, archiwa itp.
4. Należy zwracać uwagę na znajdujące się w treści wiadomości e-mail odnośniki. Jeśli wydają się nam podejrzane, to nie należy otwierać ich.
5. Użytkownikom nie wolno otwierać maili bądź załączników pochodzących z nieznanych lub nie budzących zaufania źródeł.
6. W przypadku pojawienia się wątpliwości odnośnie nadawcy bądź treści maila należy taką korespondencję przesłać do weryfikacji przez zespół IT zgodnie z wewnętrznymi procedurami

Ogólne rekomendacje bezpiecznej pracy na komputerze

1. Używanie silnych haseł.
2. Nie używanie tych samych haseł dla różnych kont i systemów.
3. Wdrożenie dwuskładnikowego logowanie wszędzie gdzie jest to możliwe.
4. Nieużywanie poczty służbowej do celów prywatnych i vice versa.
5. Postępowanie zgodnie z ustalonymi w organizacji zasadami.

6. Ograniczenie wykorzystania poczty prywatnej na urządzeniach służbowych.
7. Ograniczenie wykorzystywanie do celów służbowych chmurowych usług przechowywania plików innych niż zgodne z wewnętrzną polityką bezpieczeństwa.
8. Ograniczenie wykorzystania urządzeń prywatnych takich jak np. pamięci USB lub komórka na służbowych komputerów.

