Zasady bezpiecznej pracy przy komputerze oraz higiena pracy.

Bezpieczeństwo i higiena pracy przy komputerze, ekranie telefonu itp. pozwala zniwelować skutki wpatrywania się w monitor przez kilka godzin, co może bardzo obciążać wzrok. W przypadku siedzącej pracy przed komputerem ważny jest odpowiedni dobór mebli. Kluczowe jest, aby krzesło miało regulowaną wysokość, fotel biurowy powinien mieć także regulowane odchylenie oparcia. Odległość twarzy od monitora powinna wynosić około 40-70 cm.

Higiena pracy:

1. Aktywność fizyczna w ciągu całego dnia(gimnastyka poranna, spacer z najbliższą rodziną).
2. Odpowiednio długi sen od 7 do 11 godzin.
3. Zróżnicowane i regularne posiłki bogate w składniki odżywcze.
4. Codzienna higiena osobista całego ciała(częste mycie rąk).
5. Unikanie stresujących sytuacji.
6. Rozmowy z bliskimi.
7. Bezpieczne zachowania w domu i poza nim.
8. Odpowiednie oświetlenie stanowiska pracy.
9. Przerwy pomiędzy zadaniami-kilkuminutowe.
10. Odrabianie zadanej pracy w tym dniu w którym były zadane.
11. Ustalenie szczegółowego planu dnia.
12. Ustawienie biurka blisko okna(światło dzienne).

Podstawowe zasady użytkowania komputera, telefonu, tabletu, itp.

Należy:

- Przed przystąpieniem do pracy rozgrzać nadgarstki, palce, przedramiona,
- W pozycji siedzącej zachować naturalne krzywizny kręgosłupa i nie garbić się,
- Podpierać plecy w okolicy lędźwiowej,
- Opierać przedramiona na podłokietnikach,
- Pamiętać o tym, ze górna krawędź monitora znajdowała się na wysokości oczu lub niżej,

- Co godzinę przerywać pracę lub zabawę i odpocząć – wykonać ćwiczenia relaksacyjne lub chociaż zmienić pozycję ciała,
- Wietrzyć pomieszczenia,
- Stosować ćwiczenia relaksacyjne oczu,
- Używać okularów korekcyjnych jeśli mamy wady wzroku,

Nie należy:

- Używać sprzętu elektronicznego w skręcie tułowia,
- Ściskać kurczowo myszki, telefonu,
- Uderzać mocno w klawisze,
- Spędzać długiego czasu używając sprzętu elektronicznego

Zasady bezpieczeństwa w sieci

Do najpopularniejszych zagrożeń w cyberprzestrzeni, z którymi mogą się Państwo spotkać, należą:

- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.),
- kradzieże tożsamości, kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług,
- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne (np. phishing, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję).

Sposoby zabezpieczenia się przed zagrożeniami:

1. Korzystać z oprogramowania antywirusowego.
2. Otwierać wiadomości tylko od znajomych osób.
3. Unikać klikania w nieznane linki i załączniki w wiadomościach e-mail.
4. Ostrożnie pobierać pliki z sieci.
5. Stosować trudne do odgadnięcia hasła, które są kombinacją liter i cyfr.
6. Nie podawać w sieci danych osobowych ani haseł, nie wysyłać swoich zdjęć.

7. Chronić swoje konta na serwisach społecznościowych.
8. Czytać regulaminy.
9. Sprawdzać, czy strona, do której się logujesz, ma zabezpieczenie SSL.
10. Pamiętać, że osoba po drugiej stronie nie musi być tym, za kogo się podaje.