Kształcenie na odległość z uwzględnieniem higieny pracy oraz zasad bezpieczeństwa w sieci

informacje dla nauczycieli, uczniów i rodziców

24 marca 2020 r.

Zespół Szkół Technicznych w Nysie

Zasady bezpiecznej pracy przy komputerze

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.

Jeśli trudno jest się oderwać od komputera można pobrać darmową aplikacje dostępną w sieci np. Anti-EyeStatin lub EyeCareReminder, które pomagają zaplanować czas spędzony przed monitorem, przypomną o przerwie i zaproponują ćwiczenie oczu.

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, żeby 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

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.

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:

- zainstaluj i używaj oprogramowania antywirusowego i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym.
- Aktualizuj oprogramowanie oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie).
- Nie otwieraj plików nieznanego pochodzenia.
- Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, posiadają połączenie szyfrowane, chyba że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
- Nie używaj niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).
- Co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe – jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłające twoje hasła i inne prywatne dane do sieci

może się zainstalować na komputerze mimo dobrej ochrony – należy je wykryć i zlikwidować.

- Sprawdzaj pliki pobrane z Internetu za pomocą skanera.
- Staraj się nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu)- często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
- Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.
- Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu.
- Aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki.
- Pamiętaj o uruchomieniu firewalla.
- Wykonuj kopie zapasowe ważnych danych.
- Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.