PODSTAWOWE ZASADY BEZPIECZEŃSTWA I HIGIENY PRACY W SIECI - DLA UCZNIÓW
W SYTUACJACH KRYZYSOWYCH PRZY WYKORZYSTANIU INTERNETU - JAKO MEDIUM KOMUNIKACJI I WYMIANY TREŚCI

I. KOMINIKACJA W SIECI

- Załóż do pracy w sieci odrębny adres e-mi i posługuj się nim wyłącznie na czas pracy zdalnej w środowisku edukacyjnym obowiązującym w twojej placówce szkolnej (platformy, nauczyciele, inni uczniowie klasy-szkoły)
- Zaopatrz swój komputer w system antywirusowy i sprawdź, czy posiadasz zaktualizowane szczepionki
- Do pracy w obszarze edukacyjnym korzystaj z zaufanych połączeń do Internetu
- Zwracaj uwagę , czy strony z treściami do których odwiedzenia jesteś zachęcany mają szyfrowane połączenia z weryfikacją tożsamości dostawcy przez zaufanych wystawców protokołów tożsamości (protokół https – kłódeczka w narożniku przeglądarki/
- Nie wyłączaj zabezpieczeń domyślnych swojego komputera i sugerowanych przez system operacyjny „łat bezpieczeństwa" do zainstalowania
- Korzystaj z oprogramowania realizującego funkcję sandbox, czyli tzw. piaskownicy – zapewniając sobie bezpieczne próbowanie nowych programów, których nie znasz źródła pochodzenia. A najlepiej takich nie instaluj.
- Nie opłacaj żadnych dostępów do zasobów edukacyjnych – taka prośba przekazane mailem lub komunikatem na stronie powinna wzbudzić u ciebie podejrzenie i konieczność zakończenia połączenia
- Nie udostępniaj innym osobom swojego hasła do dedykowanych identyfikatorów na platformie edukacyjnej lub do połączeń z zasobami szkoły
- Udostępniając zasoby własnego komputera dla potrzeb innych zwracaj szczególna uwagę co faktycznie udostępniasz i z jakimi uprawnieniami - zaniechanie uwagi może się skończyć nieuprawnionym przejęciem zasobów

II. EDUKACJA W SIECI

- Korzystaj z bezpośrednio podawanych adresów pobrania oprogramowania udostępnianych na dedykowanych platformach edukacyjnych zalecanych na stronach MEN lub swojej szkoły
- Uprzednio przed połączeniem z platformą edukacyjna dane dnia pracy zdalnej dokonaj sprawdzenia parametrów jakościowych łącza – to pozwoli ci na pewność, że komunikacja w czasie kontaktu z wykładowca będzie odpowiedniej jakości i nie przerwanie dostępna.
- Jeśli proces edukacji zdalnej przewiduje przesyłanie wyników opracowań realizowanych narzędziami zainstalowanymi na twoim komputerze – staraj się dokonać konwersji do formatu PDF tuż przed wysłaniem.
- Zawsze przechowuj dokumenty źródłowe, których wysłanie było obligatoryjne w procesie oceny twojej pracy zdalnej
- Nie otwieraj plików podsyłanych mailami w formie zawartych w treści linków odsyłających do zasobów w sieci – taka forma może być początkiem przejęcia komputera lub jego zaszyfrowania / atak ransom/

Kilka proponowanych rozwiązań wartych uwagi :

- *W zakresie darmowego antywirusa : / Avast; Panda Dome; Symantec; Bitfaider*
- *W zakresie uruchomienia sandbox-a : / Windows 10 Sandbox; Sandboxie; Sandbox Avast/*
- *W zakresie przeciwdziałania atakom typu ransom : / Anti Ransom ; Trend Micro Security; Kaspersky NonRamsom /*

III. OCHRONA DANYCH i PRYWATNOŚĆ

- Dbaj o prywatność w sieci, czytaj klauzule informacyjne RODO zamieszczane przez dostawców usług
- Zapoznaj się z opisem działania mechanizmu powszechnie używanych *cookies* – pamiętaj że od ciebie zależy wyrażenie zgody na ich używanie
- Zweryfikuj ustawienia prywatności twojej przeglądarki, czy nie są czasem nadmiarowe i domyślnie zgadzasz się na fakt pobierania pewnych danych podczas połączeń, np. twojej lokalizacji
- Ogranicz do minimum wymianę danych osobowych w kontaktach z innymi przy pomocy Internetu
- Pamiętaj , że praca w oparciu o zasoby edukacyjne z twoim nauczycielem nie wymaga podawania imienia i nazwiska lub innych danych – stosuj pseudoanonimizację. Nie bądź otwarta księgą, którą czytają wszyscy …
- Jeśli posiadasz podpis elektroniczny podpisuj wysyłane dokumenty – zapewnisz sobie zachowanie integralności i udokumentowanie naruszenia twojej komunikacji
- Nie przechowuj ważnych dokumentów na dysku komputera służącego do komunikacji z wykorzystaniem Internetu. Zgraj je na dysk zewnętrzny i załóż hasło na dostęp.

Materiał nie wyczerpuje wszystkich obszarów podlegających ochronie i może być jedynie traktowany, jako zalecenie uzupełniające Politykę Bezpieczeństwa wdrożoną w organizacji .

***Robert Kozłowski**-autor opracowania*
Audytor bezpieczeństwa IT i zawodowy Inspektor Ochrony Danych
kozlowskir@cdkp.pl