TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I SZTUCZNEJ INTELIGENCJI

Część II
Cyberhigiena

Wydawnictwo: poswojsku.pl sp. z o.o.

Dariusz Gołębiowski

NOTA WYDAWCY

Wydawnictwo poswojsku.pl:

1. dołożyło wszelkich starań, by zawarte w tej książce informacje były kompletne, poprawne oraz rzetelne,
2. nie ponosi żadnej odpowiedzialności za ewentualne szkody, które mogą wyniknąć z wykorzystania informacji zawartych w tej książce.

UWAGA! Ten poradnik jest drugim w serii: Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji. Wszystkie części zawierają trzy bardzo podobne elementy: Nota Wydawcy, Od autora, Wprowadzenie do poradnika.

Wydawnictwo poswojsku.pl – kontakt:

Strona firmowa: www.poswojsku.pl

e-mail: marketing@poswojsku.pl

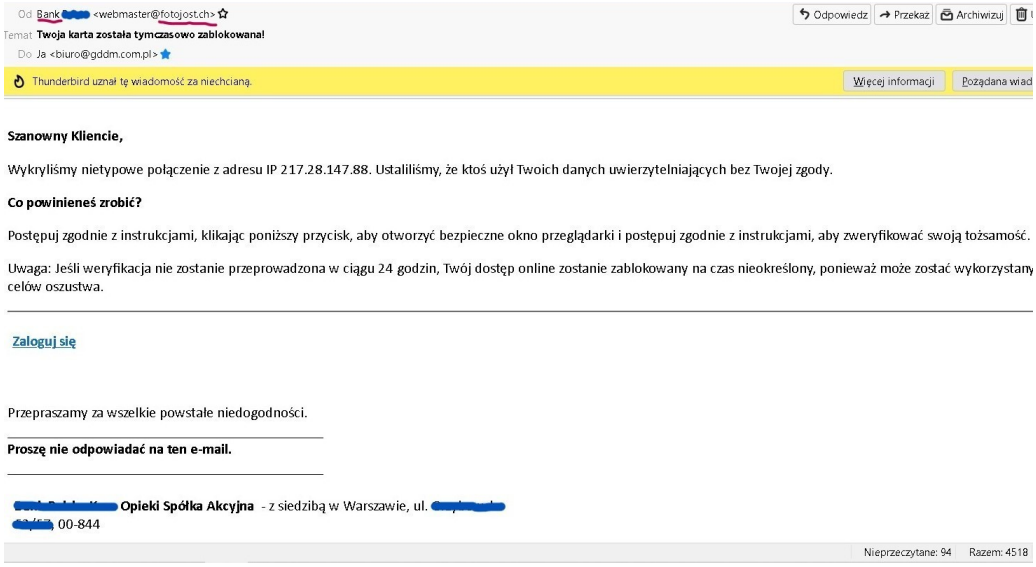
ul. Paprocka 86, 98–220 Zduńska Wola

Autor: Gołębiowski Dariusz

Zaczytaj się z poswojsku.pl – zobacz nasze propozycje wydawnicze:

TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I SZTUCZNEJ INTELIGENCJI

CZĘŚĆ II CYBERHIGIENA


Od Bank <webmaster@fotojost.ch>
Temat **Twoja karta została tymczasowo zablokowana!**
Do Ja <biuro@gddm.com.pl>
Thunderbird uznał tę wiadomość za niechcianą.
Odpowiedz | Przekaz | Archiwizuj
Więcej informacji | Pożądana wiad

Szanowny Kliencie,

Wykryliśmy nietypowe połączenie z adresu IP 217.28.147.88. Ustaliliśmy, że ktoś użył Twoich danych uwierzytelniających bez Twojej zgody.

Co powinieneś zrobić?

Postępuj zgodnie z instrukcjami, klikając poniższy przycisk, aby otworzyć bezpieczne okno przeglądarki i postępuj zgodnie z instrukcjami, aby zweryfikować swoją tożsamość.

Uwaga: Jeśli weryfikacja nie zostanie przeprowadzona w ciągu 24 godzin, Twój dostęp online zostanie zablokowany na czas nieokreślony, ponieważ może zostać wykorzystany celów oszustwa.

Zaloguj się

Przepraszamy za wszelkie powstałe niedogodności.

Proszę nie odpowiadać na ten e-mail.

Opieki Spółka Akcyjna - z siedzibą w Warszawie, ul.
00-844

Nieprzeczytane: 94 Razem: 4518

Autor: Dariusz Gołębiowski

98-220 Zduńska Wola, ul. Paprocka 86, www.gddm.com.pl,
biuro@gddm.com.pl

OD AUTORA

Witam serdecznie – Ciebie - drogi Czytelniku/czko - w poradniku "Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji: Część II – Cyberhigiena."

W obecnym świecie, w którym technologia rozwija się nieustannie, kwestia bezpieczeństwa w niezmierzonej cyberprzestrzeni staje się równie ważna, jak nasze bezpieczeństwo fizyczne. Wirtualne zagrożenia, z którymi się mierzymy – od wyrafinowanych ataków phishingowych po złośliwe oprogramowanie – wymagają od nas nie tylko zaawansowanych narzędzi obronnych, ale również podstawowej wiedzy, w tym z zakresu tzw. *higieny cyfrowej*.

W tej części poradnika wspólnie skupimy się na praktycznych aspektach cyberhigieny. Zaczniemy od metod rozpoznawania, czy padłeś/aś ofiarą cyberataku. Oczywiście mam na myśli Twoje urządzenia, typu komputer stacjonarny, smartfon, tablet, itd. Zagłębimy się także w profilaktykę cyberbezpieczeństwa, aż po metody ochrony przed coraz to nowszymi zagrożeniami. Wyjaśnię także, jak Twoje dane oraz Twoich bliskich, mogą być pozyskiwane w nieautoryzowany sposób.

Wspólnie rozważymy zagadnienie bezpiecznego przetwarzania informacji. Zastanowimy się również nad przyszłością bezpieczeństwa naszych haseł w erze sztucznej inteligencji.

Zdjęcie przedstawia wirtualne zagrożenia oraz zabezpieczenia na tle naszego wspaniałego świata rzeczywistego. Grafika została wygenerowana przy dużym udziale AI.

Część druga poradnika to także pogłębienie wiedzy o najczęściej występujących cyberzagrożeniach. Odkryjemy ludzkie aspekty stojące za atakami socjotechnicznymi, zrozumiemy mechanizmy stojące za phishingiem oraz zobaczymy, jak sztuczna inteligencja może stać się narzędziem w rękach cyberprzestępców.

Na koniec, dostarczę Tobie - sprawdzone metody ochrony przed cyberzagrożeniami. Od zasad ochrony przed atakami socjotechnicznymi, poprzez bezpieczną pracę zdalną, aż po higienę cyfrową i bezpieczne korzystanie ze sprzętu IT w podróży.

Moim celem jest wyposażenie Ciebie w wiedzę, dzięki której będziesz bezpieczne poruszać się w cyfrowym świecie, z pełną świadomością i kontrolą nad własnymi danymi. Niech ten poradnik będzie Twoją tarczą w codziennej interakcji z cyfrową technologią – otaczającą nas dookoła.

Zapraszam do lektury i odkrywania zasad cyberhigieny, które mają za zadanie chronić Twoje cyfrowe "ja".

Do zobaczenia w świecie, gdzie bezpieczeństwo i technologia idą w parze,

Dariusz Gołębiowski – Autor poradnika

Zdjęcie – Autor niniejszego poradnika w biurze, podczas: pisania, kodowania i rozmyślania ;).

Serdecznie zapraszam do kontaktu. Znajdziesz mnie bez problemu poprzez Wydawnictwo poswojsku.pl, moją stronę www, ale także na popularnych portalach społecznościowych, m.in.: Facebook, LinkedIn, youtube.com/@poswojsku .

Gdybyś szukał/a szkoleń tradycyjnych czy też on-line dla Ciebie i/lub Twojej organizacji z omawianych tutaj tematów - serdecznie zapraszam do skorzystania z moich usług ;): www.gddm.com.pl – wspaniałe, profesjonalne szkolenia oraz doradztwo z zakresu - cyberbezpieczeństwo, AI, RODO, programowanie (m.in.: Python, JavaScript, HTML, CSS, SQL).

SPIS TREŚCI Części 2 Cyberhigiena

UWAGA – w Części 1 WPROWADZENIE - znajdziesz zagadnienia:

Sztuczna inteligencja zagrożeniem czy nadzieją?

Systemy operacyjne

Linux – bezpieczeństwo

Android – najpopularniejszy OS

Windows - zabezpieczenia systemowe

Czy wszystkie przeglądarki internetowe są równie bezpieczne?

Mapy ataków cyfrowych – kolejna wojna światowa?

Rozdział 2 NARZĘDZIA DO HAKOWANIA ORAZ PODSTAWY PRAWNE

Hakowanie i hakerzy – dobro i zło

Popularne narzędzia do hakowania

AI – idealne narzędzie do hakowania

Cyberbezpieczeństwo - wprowadzenie do zagadnień prawnych

Dyrektywa NIS 2 The Network and Information Security

Ciekawe adresy świata cyber

Podsumowanie Części I

UWAGA – w Części 3 DZIECKO i TY - znajdziesz zagadnienia:

Rozdział 1

BEZPIECZEŃSTWO DZIECI W CYFROWYM ŚWIECIE

Rodzaje cyber zagrożeń w codzienności naszych dzieci

Jak rozpoznać cyberprzemoc w odniesieniu do dziecka

Rozdział 1

Cyberbezpieczeństwo w praktyce - podstawowe zasady cyberhigieny

Wizualizacja sztucznej inteligencji: Cyberhigiena jako codzienne czynności higieniczne człowieka

Jak rozpoznać, że jesteś ofiarą Cyberataku

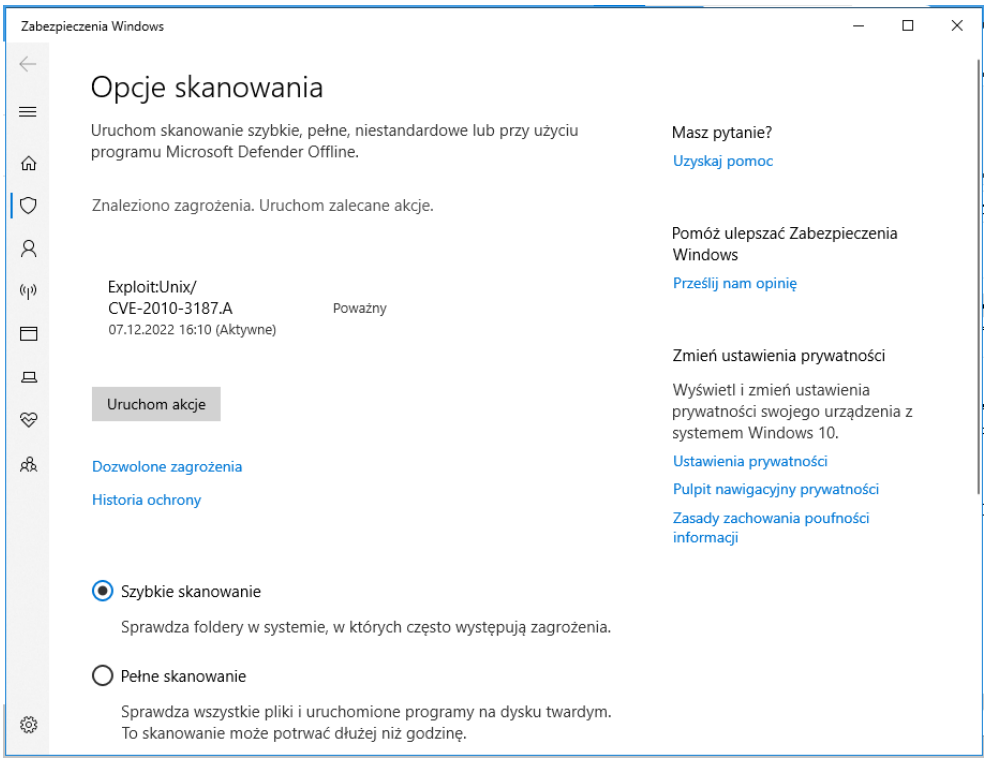
Co do bycia ofiarą ataku na Twój komputer (smartfon, tablet, laptop, itp.), to możemy mówić o dwóch rodzajach oznak:

1. ***Jawne*** – na ekranie komputera pojawia się napis, który nas informuje, że nasz sprzęt został zainfekowany jakimś zagrożeniem- np., że zostaliśmy zhakowani, jak na poniższym zdjęciu.

W tym przypadku, może pojawić się:

- stosowna informacja od zabezpieczeń systemowych posiadanych w komputerze – np. programu antywirusowego, że został znaleziony wirus.

Zdjęcie – Defaultowy program antywirusowy znalazł zagrożenie. Teraz użytkownik będzie musiał kliknąć przycisk: „Uruchom akcje" i podjąć decyzję co dalej: usunąć zagrożenie czy może skierować do kwarantanny.



Ale pamiętaj, że aby znaleźć wirusa trzeba zwykle wykonać działanie – skanowanie komputera (twardego dysku, folderów, plików, itp.). Owszem – czasami niektóre programy wychwytują wirusy będące już na Twoich dyskach. Jednakże zwykle do Ciebie należy zainicjowanie szukania zagrożeń wraz z podjęciem decyzji, co należy z nimi zrobić po ich znalezieniu (jak na powyższym zdjęciu).

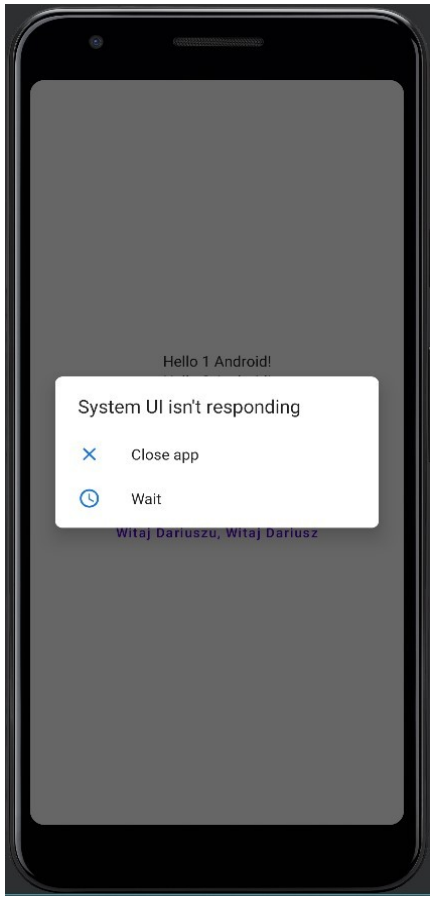
- informacje od potencjalnych napastników, dla przykładu - że został zainstalowany w naszym sprzęcie IT tzw. ransomware, czy też inne zagrożenie cyfrowe.

  Tutaj może od razu pojawić się żądanie okupu w zamian za usunięcie zagrożenia. W tym przypadku komputer zapewne jest już zablokowany. Możesz jedynie zainstalować od nowa system operacyjny i zgrać dane z kopii zapasowej lub podjąć negocjacje z przestępcami w kwestii odblokowania Twojego sprzętu. Niestety raczej nie jest to możliwe bez zapłaty okupu.

2. ***Niejawne*** – coś dziwnego dzieje się z naszym komputerem, ale nie ma żadnego jawnego komunikatu. Nawet nasze oprogramowanie antywirusowe po wykonanym skanowaniu - zupełnie milczy. Takie sygnały mogą być różnorodne. Do Ciebie należy zachować należytą uwagę i ostrożność w trakcie użytkowania Twojego urządzenia IT.

Sygnały niejawne mogące świadczyć, że jesteś ofiarą ataku hakerskiego mogą być bardzo różne. Na przykład:

- komputer działa wolniej i/lub często się zawiesza (jak na zdjęciu obok),
- na ekranie pojawiają się dziwne komunikaty, dla przykładu: reklamy jakiegoś produktu, czy strony internetowej,
- na pulpicie systemu operacyjnego zostały stworzone nowe ikony, a Ty zupełnie nie wiesz skąd się wzięły,
- przeglądarka uruchamia się sama i/lub po jej włączeniu od razu przekierowuje na nieznaną Tobie stronę,



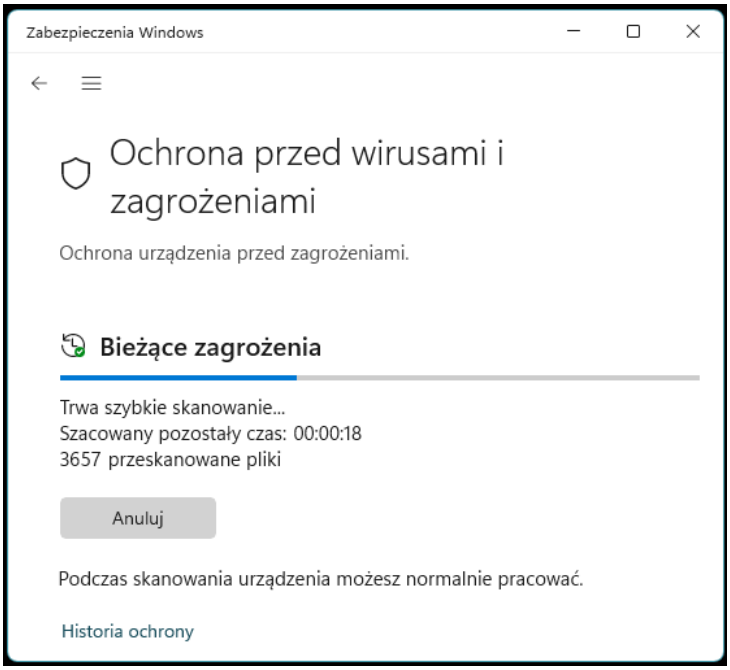
- zmieniła się struktura folderów w posiadanym systemie operacyjnym, powstały nowe foldery czy pliki - bez Twojej wiedzy i/lub zgody,

- przeglądarka ma inny wygląd, np. powstały nowe, nieznane Tobie paski narzędzi, masz wrażenie jakby to nie była Twoja przeglądarka (nie pomyl tego z nową wersją oprogramowania, zmieniającą jego wygląd – o zainstalowaniu nowej wersji, zwykle użytkownik jest informowany stosownym komunikatem),
- reklamy internetowe (w przeglądarkach czy nawet na portalach społecznościowych) nie są dopasowane do Twoich wyszukiwań oraz przyzwyczajeń, całkiem jakby ktoś inny prowadził wyszukiwania na Twoim sprzęcie komputerowym i jego oprogramowaniu.

Wyżej wymienione objawy, zapewne nie są wszystkimi możliwymi, a Ty jako odpowiedzialny użytkownik/czka komputera (stacjonarnego, laptopa, czy też urządzenia mobilnego) powinieneś/nnaś systematycznie analizować, czy danego dnia, wszystko w Twoim sprzęcie działa podobnie jak w dniach poprzednich. Codzienna czujność oraz spostrzegawczość co do ewentualnych zmian są w tym przypadku bardzo pożądane. Skoro używasz sprzętu IT, to Ty musisz spostrzec, że coś jest nie tak w jego działaniu. Przestrzegam przed podejściem nonszalanckim, typu: „Znowu ten złom się zawiesza”. Zawsze lepiej upewnić się, choćby poprzez pełne przeskanowanie systemu operacyjnego programem antywirusowym, niż przegapić jakiś incydent bezpieczeństwa.

Profilaktyka cyberbezpieczeństwa

Najbardziej istotnym elementem bezpieczeństwa – zarówno świata cyber jak i rzeczywistego, są ludzie. Każda osoba dorosła powinna zadbać o odpowiedzialne i bezpieczne używanie posiadanego sprzętu IT. A jeżeli tą osobą jest dziecko, to na jego opiekunach spoczywa ten obowiązek, choć można wiele rzeczy robić w formie zabawy razem z własnym dzieckiem. A przy okazji nabędzie ono właściwych nawyków związanych z bezpieczeństwem i ogólną higieną pracy z urządzeniami elektronicznymi.



Zdjęcie – skanowanie antywirusowe, system operacyjny Windows 11. To jest bardzo ważny nawyk w zachowaniu tzw. higieny bezpieczeństwa.

Poradnik:

Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji

Część 1 Wprowadzenie

Część 2 Cyberhigiena

Część 3 Dziecko i Ty

Zabezpiecz Swoją Cyfrową Przyszłość!

W erze cyfrowej, Twoje bezpieczeństwo online nigdy nie było ważniejsze. "Twoje cyberbezpieczeństwo w świecie cyber i AI" to Twój kompleksowy przewodnik po bezpiecznym nawigowaniu w cyfrowym uniwersum. Odkryj tajniki cyberbezpieczeństwa i zrozumienie, jak ochronić siebie i swoich bliskich przed cyberzagrożeniami, które czyhają w zaciszu cyfrowego świata.

Poznaj Fundamenty Wiedzy: Zrozumienie zagrożeń cyfrowych to podstawa. Naucz się, jakie są podstawowe pojęcia cyberbezpieczeństwa, jakie obszary są najbardziej zagrożone, i kto może być potencjalnym atakującym.

Cyberhigiena - Zasady, które Musisz Znać: Czy wiesz, jak rozpoznać, że stałeś się ofiarą cyberataku? Czy AI może złamać Twoje hasła? Dowiedz się, jakie są najlepsze praktyki cyberhigieny i jak bezpiecznie korzystać z technologii w codziennym życiu.

Ochrona Najmłodszych w Cyfrowej Dżungli: Twoje dziecko rośnie w świecie, w którym technologia jest wszechobecna. Naucz się, jak chronić najmłodszych przed cyberprzemocą i jakie są egzystencjonalne zagrożenia wynikające z interakcji z Sztuczną Inteligencją.

Narzędzia i Praktyczne Porady: Zdobądź praktyczną wiedzę o narzędziach do hakowania, zasadach ochrony przed atakami socjotechnicznymi i technicznymi, oraz o zabezpieczaniu pracy zdalnej. Plus, otrzymasz bezcenne wskazówki dotyczące bezpiecznego korzystania ze smartfonów i urządzeń IoT.

Nie pozwól, aby strach przed cyberzagrożeniami zatrzymał Cię w rozwoju osobistym i zawodowym. "Twoje cyberbezpieczeństwo w świecie cyber i AI" to broń, której potrzebujesz, aby stawić czoła wyzwaniom nowoczesnego świata.

Zainwestuj w Swoje Cyberbezpieczeństwo – Zainwestuj w Siebie – zamówienia poradnika: www.poswojsku.pl – Wydawnictwo Cyfrowe poswojsku.pl .

DZIĘKUJĘ ZA UWAGĘ :)

AUTOR:

DARIUSZ GOŁĘBIOWSKI

GDDM Potęga Wiedzy

www.gddm.com.pl