TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I SZTUCZNEJ INTELIGENCJI

Część III
Dziecko i Ty

Wydawnictwo: poswojsku.pl sp. z o.o. *Dariusz Gołębiowski*

NOTA WYDAWCY

Pamiętaj proszę: uszanuj zaangażowanie oraz godziny pracy, które spędziłem nad napisaniem oraz opracowaniem książki: TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I SZTUCZNEJ INTELIGENCJI – używaj tylko poradnik wtedy, gdy go legalnie nabyłeś/aś.

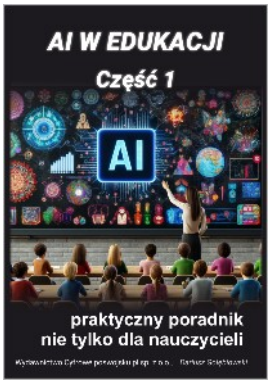
Wydawnictwo poswojsku.pl:

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.

Wydawnictwo poswojsku.pl – kontakt:
Strona firmowa: www.poswojsku.pl
e-mail: marketing@poswojsku.pl
ul. Paprocka 86, 98–220 Zduńska Wola
ISBN: 978-83-964647-8-1

Autor: Gołębiowski Dariusz

Zaczytaj się z poswojsku.pl - propozycje wydawnicze:



TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I SZTUCZNEJ INTELIGENCJI

CZĘŚĆ 3 - DZIECKO I TY

Autor: Dariusz Gołębiowski

OD AUTORA

Drodzy Czytelnicy,

Cyfrowe ślady, które codziennie zostawiamy, mogą być równie wyraźne jak nasze odciski palców. W świecie, w którym każde kliknięcie i każda interakcja online ma swoje konsekwencje, niezbędna jest świadomość, jak chronić siebie oraz swoich najbliższych – szczególnie nasze dzieci, które rodzą się po to, aby równolegle istnieć w dwóch światach: rzeczywistym i cyfrowym.

Decydując się na napisanie tej książki, a szczególnie Części 3 - chciałem stworzyć most między światem bardzo złożonych cyberzagrożeń, a codziennymi doświadczeniami milionów rodziców oraz dzieci. Część 3 - "Dziecko i Ty", to nie tylko zbiór poradników oraz wskazówek, to także zaproszenie do refleksji nad sposobem, w jaki technologia poprzez świat wirtualny kształtuje naszą wspólną rzeczywistość i wpływa na przyszłość naszych pociech.

Przedstawiam w tym poradniku, jak w prosty i praktyczny sposób zadbać o cyfrowe bezpieczeństwo rodziny, jak rozpoznać cyberprzemoc i jej przeciwdziałać. Wskazuję także - jak mądrze korzystać z kontroli rodzicielskich dostępnych na różnych platformach (systemach operacyjnych). Pragnę również zwrócić Twoją uwagę na nieoczywiste ryzyka związane ze sztuczną inteligencją. Prędzej lub później, ale na za to na pewno – staną się częścią życia Twojego kochanego dziecka.

Ten poradnik jest przeznaczony właściwie dla wszystkich – niezależnie od stopnia zaawansowania w świecie technologii. Nie potrzebujesz być ekspertem, aby zrozumieć opisane tutaj rozwiązania technologiczne. Dzięki moim poradom możesz wprowadzić zmiany, które ochronią to, co najcenniejsze – bezpieczeństwo Twoje i Twoich dzieci.

Przewodnik, który za chwilę przeczytasz, to efekt lat doświadczeń, nauki i obserwacji. Mam nadzieję, że stanie się on Twoim prywatnym kompasem w cybernetycznym świecie, który każdego dnia staje się coraz to większą częścią naszego "realnego" życia.

Podsumowując - mam nadzieję, że ten poradnik stanie się dla Ciebie niezmiernie cennym źródłem fachowej wiedzy oraz inspirujących pomysłów, które spowodują, że Ty i Twoja rodzina będziecie bardziej bezpieczni w świecie cyber.

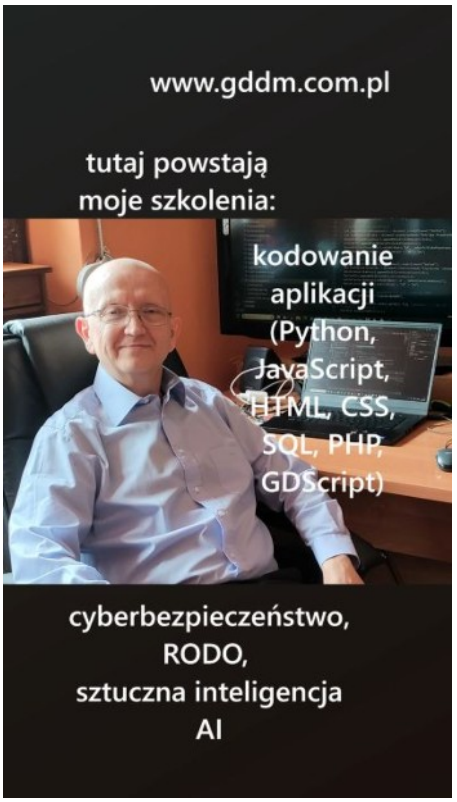
Z wyrazami szacunku:

Dariusz Gołębiowski

Autor poleca

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

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



WPROWADZENIE DO CZĘŚCI 3

Żyjemy w niesamowitej erze cyfrowej, gdzie granice między światem online a offline zacierają się z dnia na dzień. Nasze urządzenia stały się czymś w rodzaju przedłużenia nas samych. Są to narzędzia wielozadaniowe. Mogą służyć do: pracy, nauki, zabawy. Często robią za tzw. „zabijacze czasu". Wiele osób, gdy się nudzi lub jest zmęczonych to po prostu … klika :). Jednakże, jak wszystkie narzędzia, mogą być one źródłem niebezpieczeństwa. Szczególnie, gdy zostaną użyte nieumiejętnie czy też po prostu w głupi, nieodpowiedzialny sposób. Dlatego właśnie powstał ten poradnik. Chcę dać Wam – Drodzy Czytelnicy - narzędzia, wiedzę i świadomość, niezbędne do bezpiecznej nawigacji w cyfrowym świecie. I to zarówno dla Ciebie, jak i Twoich kochanych dzieci.

Pozwól, że na początku napiszę kilka słów, na temat kolejnych rozdziałów tej książki, nad którymi wspólnie się pochylimy.

Rozdział 1: Bezpieczeństwo dzieci w cyfrowym świecie

W pierwszym rozdziale zajmiemy się tym, co jest fundamentem naszego codziennego spokoju – bezpieczeństwem naszych dzieci online. Dowiesz się o różnych rodzajach cyfrowych zagrożeń, które czyhają na Ciebie i Twoich bliskich w internecie oraz o tym, jak je rozpoznać. Otrzymasz praktyczne porady pomagające w rozwiązaniu wielu problemów związanych z cyberbezpieczeństwem i AI. Najważniejsze zagadnienia wypunktowałem poniżej.

- Jak dbać o bezpieczeństwo cyfrowe najmłodszych, równocześnie nie zapominając o kontroli rodzicielskiej w różnych systemach operacyjnych.
- Jak rozpoznać cyberprzemoc w odniesieniu do dziecka. Pamiętaj: zapobiegaj zamiast leczyć, ale czasami już nie da się chronić dziecka przed zagrożeniem. Trzeba potrafić je skutecznie rozpoznać i pomóc córce/synowi w rozwiązaniu cyfrowego problemu.
- Co to jest kontrola rodzicielska i jak ją skutecznie wdrożyć. Omówię kilka systemów operacyjnych.
- Poruszę także kwestię sztucznej inteligencji i jej wpływu na dzieci. Krótko omówimy najważniejsze zagrożenia dla najmłodszych związane z AI, które mogą nie być od razu widoczne.

Rozdział 2: Twoje bezpieczeństwo w cyfrowym świecie

Twoje bezpieczeństwo jest równie ważne, co Twoich bliskich. Przecież jesteś wzorem, przykładem zachowania w świecie cyber dla całej rodziny oraz najbliższych. A przynajmniej tak być powinno :).

W tym rozdziale wskażę m.in.:

- Jak bezpiecznie pobierać zdjęcia oraz inne zasoby z internetu.
- Dowiesz się także jak należy postępować, gdy wydarzy się nieszczęście i padniesz ofiarą cyberataku.
- Wspólnie przejdziemy przez sekrety tworzenia i przechowywania bezpiecznych haseł.
- Omówimy także metody szyfrowania danych, które dodadzą kolejną warstwę ochrony Twojej prywatności. Skupimy się w tym zakresie na bezpłatnym oprogramowaniu do szyfrowania, typu: 7Zip i VeraCrypt. Są to niezbędne narzędzia w arsenale każdego użytkownika internetu.

MOTTO:
ZAPOBIEGAJ ZAMIAST LECZYĆ - !!!!
od rozmowy - poprzez aktywne czynności
do bezpieczeństwa Twojego dziecka

SPIS TREŚCI

Rozdział 2

Rozdział 1

BEZPIECZEŃSTWO DZIECI W CYFROWYM ŚWIECIE

RODZAJE CYBERZAGROŻEŃ W CODZIENNYM ŻYCIU NASZYCH DZIECI

Istniej wiele rodzajów cyberzagrożeń dla dzieci, które mogą prowadzić do bardzo poważnych konsekwencji dla:

- dzieci,
- rodzin,
- społeczeństwa, w tym społeczności szkolnej.

Pozwól, że wymienię kilka najważniejszych cyfrowych niebezpieczeństw.

CYBERPRZEMOC

Jest to bardzo ogólne pojęcie, pod którym może się kryć wiele różnych, złych czynów. Między innymi przemoc dokonywana za pośrednictwem:

- sieci www

  (portale społecznościowe, gry internetowe, fora tematyczne, itp.),
- urządzeń elektronicznych

  (smartfony, komputery stacjonarne, laptopy, tablety, konsole do gier, itp.).

Cyberprzestępcy wykorzystują nowoczesne technologie teleinformatyczne (informacyjne oraz komunikacyjne) do wyrządzania krzywdy pojedynczym osobom i/lub całej grupie. Zazwyczaj przemoc przybiera wymiar:

- psychiczny,
- społeczny,

ale może prowadzić do negatywnych skutków także w świecie realnym – wymiar fizyczny. Bardzo często cyberprzemoc jest przejawem agresji rówieśniczej.

Obecnie z cyberprzemocą silnie związany jest rozwój sztucznej inteligencji. Z wykorzystaniem AI powstają różnorodne nieprawdziwe, czyli „fakowe" informacje, które mogą np. ośmieszać dane dziecko czy całą grupę małoletnich osób. Technologia sprzyja w tym przypadku szerzeniu się tzw. wiadomości fakowych. A niestety nie ma narzędzi, które jednoznacznie wskazywałyby, czy dana wiadomość tekstowa, graficzna czy multimedialna – jest prawdziwa czy też tylko wygenerowana przez AI. Jeżeli ten stan rzeczy utrzyma się dłużej, to możemy być świadkiem wielu tragedii. Zarówno wśród dzieci jak i osób dorosłych.

GROOMING

jest to proces, w ramach którego osoba dorosła nawiązuje relację z dzieckiem w celu wykorzystania go (zwykle) seksualnie. Mogą to być dla przykładu:

- członkowie rodziny,
- tzw. „przyjaciele rodziny",
- nauczyciel/ka,
- znajomy/a,
- osoba obca – dla przykładu poznana w internecie.

Grooming

etapy przestępczej działalności:

- Poznanie dziecka - zdobycie zaufania, wysłuchanie problemów, oferowanie pomocy.
- Budowanie więzi wirtualnej - zbliżenie się do dziecka, bycie przyjacielem, przyjaciółką, a nawet zaufanym powiernikiem najbardziej prywatnych informacji.
- Kontakt fizyczny – zwykle świadczenie jakiegoś rodzaju pomocy dla nieświadomego, zagubionego psychicznie dziecka.
- Znajomość intymna - poruszanie tematów o charakterze seksualnym, uczenie dziecka o seksie, stwarzanie okazji do intymnych spotkań.
- Wykorzystanie seksualne - często stosując przemoc, szantaż czy groźby.
- Uprowadzenie a nawet zabójstwo – aby ukryć swoje czyny, przestępca - groomer, może tym skrajnym etapem zakończyć proces manipulowania młodocianą osobą.

Jak rozpoznać grooming?

Aby rozpoznać grooming, trzeba przede wszystkim zwrócić uwagę na codzienne zachowanie młodej osoby. I tutaj pojawia się problem, bo zajęci sprawami życia codziennego rodzice, mogą przegapić istotne zmiany w sposobie zachowania swojej pociechy. W obecnym konsumpcyjnym społeczeństwie, niejednokrotnie brak czasu poprzez np. zajęcie karierą zawodową, powoduje, że obca osoba wie więcej o dziecku niż jego rodzice. Niestety, niejednokrotnie prowadzi to do tragedii, gdyż obca osoba przejmuje kontrolę, którą powinni sprawować nad dzieckiem prawni opiekunowie. Można by tego uniknąć, gdyby tylko okazać więcej zainteresowania własnemu dziecku.

Na co więc rodzice powinni zwrócić uwagę?

Rodzice powinni zwrócić uwagę na zachowanie swojej pociechy. Czy dziecko:

- jest tajemnicze,
- nie chce rozmawiać o internecie,
- staje się agresywne/wycofane,
- otrzymuje od osoby dorosłej prezenty, pieniądze, czy inne korzyści,
- otrzymuje od osoby dorosłej wiadomości o niewłaściwym charakterze (np. z podtekstem seksualnym),
- umawia się z osobą dorosłą na fizyczne spotkanie.

Grooming może prowadzić do bardzo wielu nieszczęść młodej osoby, ale także całego jej bezpośredniego otoczenia. Lecz przede wszystkim stanowi on bezpośrednie zagrożenie dla zdrowia oraz życia dziecka w wymiarach:

- fizycznym,
- psychicznym.

Poza GROOMINGIEM istnieje wiele innych groźnych zagrożeń. Oto niektóre z nich.

Sexting

Przesyłanie lub upublicznianie w sieci internet, ale także za pomocą technologii SMS - prywatnych zdjęć i/lub filmów, które ukazują rozneglіżowaną a czasami wręcz nagą ofiarę. Do tego bardzo często dochodzą różnego rodzaju wiadomości o zabarwieniu erotycznym.

Tutaj możemy mieć do czynienia także z wyprodukowaniem za pomocą AI zupełnie fałszywych zdjęć, filmów, itp. Jak już wspomniałem, na dzień dzisiejszy nie ma praktycznie żadnej ochrony przed tego typu zagrożeniem.

Cyberstalking

Uporczywe nękanie oraz śledzenie działań ofiary za pomocą Internetu. Bardzo często przenosi się także do świata realnego prowadząc do prześladowania osoby poszkodowanej.

Oszustwa internetowe

Próby wyłudzenia środków finansowych i/lub danych osobowych ofiary przez osoby podszywające się pod: przyjaciół, znajomych, znane osoby świata rzeczywistego, instytucje finansowe, sklepy internetowe, czy też inne osoby. Dzieci, jako najmniej doświadczone elementy ludzkiego społeczeństwa, są szczególnie mocno narażone na działania przestępcze tego typu, gdyż są zwykle dużo łatwiejszym celem niż osoby dorosłe.

PODSUMOWANIE

W dzisiejszym dynamicznie rozwijającym się cyfrowym świecie, bezpieczeństwo nasze oraz naszych dzieci staje się kwestią priorytetową. Znajomość zagrożeń i umiejętność ich przeciwdziałania to podstawa, o której mówi ten poradnik. Bezpieczeństwo cyfrowe to nie tylko ochrona przed cyberprzestępcami, ale również świadome korzystanie z zasobów internetu.

Nasze kochane dzieci, wychowując się w erze cyfrowej, są szczególnie narażone na różnorodne zagrożenia. Wiedza o tym, jak rozpoznać oraz przeciwdziałać cyberprzemocy, jak również zarządzanie ustawieniami prywatności i kontrolą rodzicielską na różnych systemach operacyjnych, stanowi istotną tarczę ochronną. Zarówno Windows, Linux, jak i Android oferują narzędzia, które, stosowane prawidłowo, mogą znacząco zwiększyć bezpieczeństwo naszych pociech.

Sztuczna inteligencja, choć otwiera przed nami nowe możliwości, również rodzi nowe wyzwania. Zrozumienie potencjalnych zagrożeń egzystencjalnych związanych z AI to klucz do odpowiedzialnego wprowadzania dzieci w ten świat.

Dorośli, z kolei, muszą być świadomi ryzyka związanego z utratą danych czy dostępu do kont społecznościowych. Wiedza o tym, jak bezpiecznie pobierać zdjęcia i inne zasoby z internetu, jak zarządzać hasłami za pomocą takich narzędzi jak KeePass, czy korzystać z metod szyfrowania dysków i plików przy użyciu VeraCrypt, to fundamenty, które pomogą zabezpieczyć Twoją cyfrową tożsamość.

W tym poradniku podkreśliłem również znaczenie sprawdzania poprawności ściąganych plików, co jest prostym, ale skutecznym sposobem na uniknięcie złośliwego oprogramowania.

Podsumowując, dobrze byłoby gdybyś ten poradnik potraktował/a, jako przewodnik po cyfrowym świecie, który w coraz większym stopniu wpływa na wszystkie aspekty naszego życia. Rozwój technologiczny jest nieunikniony, ale z odpowiednią wiedzą oraz narzędziami, możemy kształtować ten świat tak, aby był bezpieczny dla nas i naszych dzieci. Bezpieczeństwo cyfrowe to nie tylko technologia, to przede wszystkim odpowiedzialność, świadomość, rozsądek oraz ciągła edukacja. Pamiętaj, że w świecie cyfrowym, podobnie jak w realnym, najważniejsza jest współpraca, wzajemny szacunek i dbałość o dobro wspólne.

Serdecznie dziękuję za uwagę i pozdrawiam
Dariusz Gołębiowski

PODZIĘKOWANIA

Serdecznie dziękuję za zapoznanie się z zawartością mojego poradnika. Mam nadzieję, że przyniósł on Tobie Droga Czytelniczko/ Wspaniały Czytelniku - dużo wiedzy oraz zrozumienia odnośnie sposobów efektywnego uniknięcia cyfrowych zagrożeń dla Ciebie oraz całej Twojej rodziny oraz znajomych.

Zapraszam Ciebie także do poznania także pozostałych części mojej serii „Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji", która obecnie składa się z:

CZĘŚĆ I WPROWADZENIE

CZĘŚĆ II CYBERHIGIENA

CZĘŚĆ III DZIECKO I TY

W Częściach 1 i 2 mojego poradnika znajdziesz zagadnienia:

W poradniku wykorzystano:

- własne materiały graficzne,
- prace graficzne: Chat GPT4,
- cliparty z programu LibreOffice na licencji CCO.

DZIĘKUJĘ ZA UWAGĘ

Autor poradnika: DARIUSZ GOŁĘBIOWSKI

Zapraszam do zapoznania się z innymi książkami, które napisałem lub współtworzyłem.

Więcej informacji znajdziesz na stronach firmy:

Wydawnictwo Cyfrowe poswojsku.pl , www.poswojsku.pl