CYBER AWARE

CZYLI

podręcznik świadomego użytkownika cyberprzestrzeni:
bezpieczeństwo, AI i dezinformacja

CyberAware, czyli podręcznik świadomego użytkownika cyberprzestrzeni: bezpieczeństwo, AI i dezinformacja

I
Wprowadzenie do cyberbezpieczeństwa

1. A co to takiego to cyberbezpieczeństwo?

Zacznijmy naszą przygodę od podstaw. Najpierw przecież trzeba dowiedzieć się czym jest pojęcie, w które będziemy się wgłębiać.

Cyberbezpieczeństwem nazywamy techniki, procesy i praktyki stosowane do ochrony różnorakich urządzeń, programów, danych i sieci komputerowych. Jest ono szczególnie ważne w dzisiejszych czasach, gdzie prawie wszystko kontrolowane jest jakiegoś rodzaju komputerem. Masa usług i firm całkowicie polega na dostępie do Internetu.

A teraz to co robicie?

Czytacie ten tekst pewnie na jakimś telefonie, komputerze, czy innego rodzaju urządzeniu, które Wam to umożliwia.

A co nam będzie potrzebne w tej cyfrowej przygodzie?

Otóż kilka podstawowych pojęć. Założymy się, że wszystkie znacie. My natomiast wprowadzimy trochę fachowego języka.

- **Atak hakerski**

Nazywamy tak działania, które mają na celu przejęcie kontroli nad jakimś urządzeniem albo pozyskaniem z niego przydatnych, czy wartościowych danych.

- **Malware,** a prościej - złośliwe oprogramowanie

To programy stworzone, aby ułatwić lub umożliwić przeprowadzenie ataku hakerskiego (wirusy, trojany, itp).

- **Antywirus**

Oprócz tego, że jego darmowe wersje grają nam często na nerwach, to jest to przydatne oprogramowanie, które wykrywa złośliwe programy na komputerze i pozwala na ich usunięcie.

- **Firewall**, zwana też zaporą sieciową

To oprogramowanie lub urządzenie, które pozwala na określenie, jaki ruch w sieci jest dozwolony, czyli pomaga kontrolować operacje w niej wykonywane, co zmniejsza ryzyko ataku hakerskiego.

2. Jakie niebezpieczeństwa czyhają na nas w sieci?

Największym zagrożeniem w dzisiejszym Internecie zdecydowanie są **oszustwa**.

A dlaczego tak jest?

Nowoczesne systemy komputerowe są na tyle bezpieczne, że bardzo ciężko jest się do nich włamać bez ingerencji użytkownika danego urządzenia. Na marginesie, taki rodzaj ataku, gdzie wykorzystuje się osobę korzystającą z danego systemu do przejęcia nad nim kontroli nazywamy socjotechniką.

Zatem, w jaki sposób najczęściej działają oszuści? Techniki te mogły wam obić się o uszy, my wyjaśniamy na czym dokładnie polegają.

- **Phishing**

To technika, w której tworzona jest sztuczna strona, udająca witrynę logowania do prawdziwego serwisu.
Gdy podasz na niej swoje dane, przesyłane są one do hakera.
Często linki do takich stron wysyłane są poprzez e-mail lub SMS, gdzie atakujący podszywa się pod firmę lub instytucję, z której usług korzysta dana osoba. Wtedy klikając w taki link otworzy ci się okienko z fałszywą witryną.

- **Vishing**

To rodzaj ataku phishingowego, jest on przeprowadzany przez połączenie telefoniczne (haker dzwoni do ofiary i podszywa się za np. bank).

- **Oszustwo inwestycyjne**

Oszust wmawia ofierze, że może błyskawicznie zarobić duże pieniądze. Naciska, twierdząc, że to wyjątkowa okazja, która zaraz zniknie. Gdy ofiara uwierzy, może żądać kolejnych wpłat, udając, że to konieczne do wypłaty tego co zdobyła na inwestycji.

- **Złośliwe oprogramowanie**

Dzięki niemu haker namawia ofiarę do uruchomienia programu, który umożliwi mu dostęp do pożądanych przez niego zasobów, np. danych.

Na szczęście, w dzisiejszych czasach nie musimy się aż tak przejmować złośliwym oprogramowaniem jak kiedyś, dzięki rozwojowi antywirusów. System Windows, którego na komputerach używa większość z was ma domyślnie zainstalowany i uruchomiony wystarczający program, który chroni wasze sprzęty.

Pamiętajcie jednak, że nie zawsze wykrywają one wszystkie zagrożenia. Musicie nadal zachować szczególną ostrożność, gdy pobieracie różne programy z Internetu, czy z załączników wiadomości e-mail.

W takim razie nadszedł czas by poznać rodzaje złośliwego oprogramowania i w jaki sposób działają.

Oto parę z nich:

- **Trojan** - haker po cichu może kontrolować wasze urządzenie, ponieważ Trojan udaje inne oprogramowanie, przez co może być dla nas niezauważalny.
- **Wirusy** - po włączeniu urządzenia przyczepiają się do programów i próbują rozprzestrzeniać się na inne urządzenia w sieci.
- **Ransomware** - szyfruje dane na dysku i żąda opłaty za to by zostały odszyfrowane.
- **Adware** - wyświetla reklamy na urządzeniu.
- **Spyware** - działa w tle, zajmuje się zbieraniem informacji o użytkowniku.

II
Sztuczna inteligencja w pracy i edukacji

1. Sztuczna Inteligencja jako partner w pracy: narzędzia i aplikacje w praktyce

W dobie szybko rozwijającej się Sztucznej Inteligencji (AI) pewnie ktoś z was się zastanawiał, jak może ją wykorzystać w szkole lub pracy. Powstało już dużo takich narzędzi wykorzystujących tą technologię w tych dziedzinach, jednak zawsze trzeba uważać i weryfikować odpowiedzi, które od nich otrzymujemy.

Taki stan rzeczy spowodowany jest przez to, że AI nie może weryfikować swojej wiedzy i nie może nam powiedzieć, że czegoś nie wie. Zamiast tego zdarza się, że zwraca po prostu kłamstwa.

W szkole i pracy przydatne mogą się okazać narzędzia związane z **tworzeniem jakiegoś tekstu**. Znaleźliśmy kilka takich programów:

- **Grammarly**

Sprawdza na bieżąco pisownię, gramatykę, interpunkcję, składnię (budowę zdania) i przejrzystość. Może też sugerować zmiany w strukturze i stylu zdań, które polepszą czytelność tekstu.

- **Hemingway Editor**

Skupia się na przejrzystości i łatwości czytania. Wyróżnia złożone zdania oraz trudne do zrozumienia części. Daje sugestie, jak uprościć nasz tekst, zaznaczając słowa i fragmenty, nadające się do poprawki.

Do nauki może przydać się program **Khanmigo**.
To asystent AI stworzony przez Khan Academy. Jego zaletą jest to, że dostosowuje się do poziomu umiejętności ucznia, podaje wskazówki na temat konkretnych zadań i tłumaczy błędy.
Działa w sposób interaktywny, więc nauka może stać się ciekawsza, a przy tym przyjemniejsza i szybsza.
Czy nie brzmi zachęcająco? Przecież skrócenie czasu spędzonego nad książkami to miód na nasze i wasze serce.

Khanmigo może być wykorzystany także przez nauczycieli. Dzięki niemu w łatwy sposób można stworzyć plan zajęć, czy przygotować na nie materiały.

Dla programistów i fanów **programowania** też coś mamy:

- **Github CoPilot**

To asystent AI, który pomaga programować szybciej, wkładając w to mniej wysiłku. Daje sugestie kodu, odpowiada na pytania, a nawet potrafi opisać co się zmieniło od ostatniego zapisania pracy.

- **Środowiska programistyczne JetBrains**

Takie jak PyCharm, IntelliJ IDEA czy PhpStorm, mają wbudowaną sztuczną inteligencję. Pomaga ona w programowaniu – podpowiada poprawki, wyjaśnia błędy, opisuje zmiany od ostatniego zapisania i tłumaczy, jak działa kod.

2. Sztuczna inteligencja wokół nas – czy naprawdę jej nie zauważamy?

Wróćmy jednak do początków - skąd w ogóle pomysł na sztuczną inteligencję?

Ludzkość od zawsze myślała o stworzeniu dla siebie asystentów, które będą jej ułatwiać wykonywanie różnorakich czynności. Idea AI sięga starożytnej Grecji – w mitologii bóg Hefajstos stworzył mechaniczne służebnice ze złota, które pomagały mu w codziennych obowiązkach.

Wydaje się, że sztuczna inteligencja nie ma bardzo dużego wpływu na nasze życie. Ale czy na pewno?

Ogromna ilość serwisów, które używamy, po cichu wykorzystuje AI w tle. Przykładem tego są **algorytmy polecania treści** w mediach społecznościowych lub w serwisach streamingowych takich jak Netflix lub Spotify. Znacie już podobne mechanizmy z poprzedniego rozdziału - dane, które zbierają o nas różne organizacje są przecież wykorzystywane też do personalizacji reklam. Dokładność, z jaką treści są nam rekomendowane potrafi być aż niepokojąca.

Aktualnie rozwijane są systemy pozwalające **samochodom** na jeżdżenie z coraz mniejszą ingerencją kierowcy. Największą popularnością cieszy się rozwiązanie marki Tesla, która chce zaoferować w ich pojazdach autopilota.

Jednak większość znanych marek posiada w swoich samochodach funkcje, które wykorzystują AI - przykładowo BMW, Mercedes, GM oraz Ford.

Wirtualni asystenci, tacy jak ChatGPT lub Deepseek szybko stają się coraz to bardziej powszechne w naszej codzienności. Mogą pomagać nam w wielu zadaniach, a szczególnie wyróżniają się w szybkiej redakcji i poprawianiu błędów w tekstach. Trzeba jednak zachować dużą ostrożność, używając tych narzędzi. Jak wcześniej wspomnieliśmy - mogą robić błędy, bo naturalnie nie zdają sobie z nich sprawy.

III

Dezinformacja w cyberprzestrzeni

1. Dlaczego musimy być czujni?

Patrząc na nazwę łatwo się domyślić, że dezinformacja ma na celu przekazanie nam pewnej wiadomości, która **nie jest prawdziwa**. To bez wątpienia działanie, które ma specjalnie wprowadzić nas w błąd lub przekonać do podjęcia jakiejś decyzji, czy zmianę naszego poglądu na dany temat - takie zjawisko nazywamy manipulacją informacyjną.

Rozwijająca się technologia sprzyja powstawaniu nowych form dezinformacji. Spotkać ją możemy teraz dosłownie wszędzie. Najczęściej do jej rozpowszechniania używa się fałszywych wiadomości, przerobionych zdjęć lub filmów, a nawet sfałszowanych dokumentów.

W dobie Internetu jest ona coraz większym problemem. Często ciężko się połapać, co jest kłamstwem, a co prawdą.

Zatem w jakiej postaci możemy się na co dzień natknąć na dezinformacje? Oto parę przykładów:

- **Fake news** - fałszywe wiadomości, na przykład o katastrofach lub wydarzeniach politycznych.
- **Przerobione, edytowane zdjęcia** - pokazują coś, co nigdy się nie wydarzyło.
- **Deepfake** – użycie sztucznej inteligencji do wygenerowania bardzo prawdziwie wyglądających, ale nieprawdziwych nagrań wideo lub dźwiękowych, np. podrabianie czyjegoś głosu.

Skutki tego typu działań możemy wyraźnie odczuć w otaczającym nas środowisku - rozmawiając ze znajomymi, słuchając rozmów, rodzinnych dyskusji, które często zahaczają o to co, kto i gdzie wyczytał w Internecie.

Przez dezinformację ludzie tracą zaufanie do mediów, różnych instytucji, organizacji, a w skrajnym przypadku nawet do samych siebie. Wśród nas kształtują się skrajne opinie i poglądy (np. polityczne), które prowadzą do polaryzacji społeczeństwa.

Fałszywa informacja może wpłynąć także na nasze działanie, podjęte często pod wpływem skrajnych emocji (strachu, paniki i nie tylko), które wywołała.

2. W świecie fałszywych informacji – jak media społecznościowe zniekształcają rzeczywistość.

Platformy społecznościowe są najczęstszym źródłem dezinformacji. Wynika to z faktu, że obecnie niemal każdy ma do nich dostęp. Można na nich niemal bez ograniczeń zamieszczać treści, które błyskawicznie się rozprzestrzeniają.

Ponadto dużą rolę odgrywa względna **anonimowość** w Internecie. Korzystając z mediów społecznościowych, bardzo łatwo podszyć się pod osobę wzbudzającą zaufanie publiczności – na przykład specjalistę, lekarza czy ogólnie osobę wykształconą.

Obecnie dużą rolę odgrywają internetowi celebryci – **influencerzy**. Fani przeważnie traktują ich jako autorytety, a co za tym idzie – darzą ich zaufaniem. Wielu z nich zdobyło sławę bardzo szybko, nie zdając sobie sprawy, że wiąże się ona z dużą odpowiedzialnością. Ich posty docierają do ogromnej liczby odbiorców, dlatego powinni starannie dobierać promowane treści.

Rzeczywistość jednak nie jest aż tak kolorowa.

Gdy dotrą do nas fałszywe treści i zaczniemy wchodzić z nimi w interakcję (polubimy wątek, napiszemy komentarz), algorytm platformy stopniowo zacznie pokazywać nam coraz więcej postów nagłaśniających podobne poglądy. Tego typu platformy są zaprojektowane tak, aby przyciągnąć naszą uwagę na jak najdłużej. Osiągają to poprzez precyzyjny dobór i rekomendowanie materiałów, które nas zainteresują lub z którymi będziemy się zgadzać.

To zjawisko stało się na tyle powszechne, że zyskało nawet własną nazwę:

„**Echo chamber**” – stan, w którym jesteśmy otoczeni wyłącznie informacjami zgodnymi z naszymi poglądami.

Jest skrajnie niebezpieczny i szybko prowadzi do zamknięcia się na odmienne opinie oraz do zwiększenia przekonania o własnej racji. Po pewnym czasie może to całkowicie uniemożliwić dyskusję z osobami o odmiennych poglądach. Próba podjęcia rozmowy często kończy się agresją i frustracją.

IV
Rozpoznawanie dezinformacji

1. Jak rozpoznać dezinformację w sieci?

Rozpoznawanie nieprawdziwych treści w sieci z dnia na dzień staje się coraz ważniejszą umiejętnością. Żyjemy w czasach, w których nie możemy całkowicie ufać żadnemu źródłu. Niestety, nie jest to zawsze łatwe - wymaga to od nas większego wysiłku i zaangażowania zdeczka więcej czasu. A co najważniejsze, nie wiemy często jak się w ogóle za to zabrać.
A więc - jak?
To kilka sposobów, które dla was znaleźliśmy:

1. Gdy zobaczycie jakąś informację w mediach społecznościowych warto poszukać jej **pierwotnego źródła**, czyli takiego, które jako pierwsze podało daną wiadomość.
2. Weryfikacja **autentyczności kont**, które zamieszczają jakieś informacje, ponieważ często zdarza się, że osoba je publikująca parodiuje (wyśmiewa się) kogoś lub coś, albo nie ma odpowiednich kwalifikacji by je podawać.
3. Starajcie się **nie używać tylko jednego źródła** informacji - to otworzy was na odmienne opinie i poglądy, pomoże uchronić przed zjawiskiem, którym jest “echo chamber”, wspomnianym w poprzednim rozdziale.
4. **Fact-checking** (weryfikacja faktów) to proces sprawdzania prawdziwości informacji, aby upewnić się, że są zgodne z rzeczywistością. Składają się na niego wymienione wyżej sposoby.
5. Istnieją **organizacje**, które profesjonalnie zajmują się weryfikacją tego co pojawia się w sieci. Gdy ustalą, że dana informacja jest wiarygodna - publikują ją.

A co najważniejsze - większość z tego co czytacie w Internecie powinniście traktować jako nieprawdę, dopóki nie sprawdzicie rzetelności tych informacji.

2. Analiza przypadków:

Największe skandale dezinformacyjne.

Skutki dezinformacji nie kończą się w Internecie - potrafi mieć ona poważne konsekwencje w realnym świecie.

Jej cechą charakterystyczną jest wzbudzanie ekstremalnych uczuć, takich jak agresja, czy panika w społeczeństwie. W ostatnich latach przeżyliśmy już wiele sytuacji wywołanych fałszywymi informacjami - to znak by wyciągnąć z nich wnioski.

Po **wyborach prezydenckich w USA w 2020 roku** internet zalała fala teorii spiskowych – wybory miały być sfałszowane. Nie było na to żadnych dowodów, ale nie powstrzymało to lawiny dezinformacji. Plotki i manipulacje rozprzestrzeniały się błyskawicznie, podsycając napięcie polityczne w kraju.
Kulminacją tego chaosu był 6 stycznia 2021 roku, gdy tłum zwolenników teorii spiskowych szturmował Kapitol. Świat patrzył w osłupieniu, gdy budynek – symbol amerykańskiej demokracji – został oblężony. W ciągu 36 godzin od ataku zginęło pięć osób, a 174 policjantów zostało rannych. Tragiczne skutki nie skończyły się tego dnia – w kolejnych miesiącach czterech funkcjonariuszy, którzy brali udział w obronie Kapitolu, popełniło samobójstwo.
Skala zniszczeń była ogromna – szkody materialne oszacowano na ponad 2,7 miliona dolarów. Jednak prawdziwe straty były o wiele większe – nadszarpnięte zaufanie do demokracji, podziały społeczne i niepokój, który jeszcze długo nie opuścił Stanów Zjednoczonych.

W tym czasie szalała dodatkowo jeszcze **pandemia COVID-19**, która stała się wylęgarnią teorii spiskowych i przepisów na fałszywe “lekarstwa”. Takie zjawisko nazwano “**dezinfodemią**” - jak łatwo się domyślić - pandemią dezinformacji.
Popularną narracją była teoria, że wirus był bronią biologiczną, która wyciekła z laboratorium. Co więcej, w różnych częściach świata o wywołanie globalnego kryzysu oskarżano różne państwa, czy grupy etniczne.

Najgroźniejsze dla ludzi, z pewnością okazały się rozprzestrzeniające domowe sposoby na zwalczanie wirusa. Znaczna większość była nieszkodliwa (np.

suplementacja witaminy C lub picie ciepłych napojów), ale rosła też popularność takich, których skutki zagrażały zdrowiu, a nawet życiu.

Powstała plotka, że alkohol może działać zapobiegawczo przed zachorowaniem na COVID, co skończyło się drastycznym wzrostem ilości zatruć metanolem, którego produkty rozkładu są silnie toksyczne dla organizmu człowieka.

Niebezpieczne mity nie kończyły się jednak na alkoholu. W sieci krążyły także teorie, że palenie tytoniu lub wdychanie kokainy może zapobiec zakażeniu. Choć brzmi to jak żart, wiele osób traktowało te informacje poważnie, ryzykując własnym zdrowiem.

V
Cyberbezpieczeństwo w praktyce

1.Ochrona przed cyberzagrożeniami – co musisz wiedzieć?

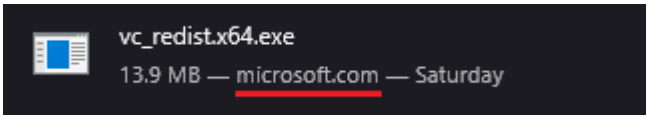
Bezpieczeństwo w Internecie to podstawa.

Wiele z was pewnie twierdzi, że to trudne i strasznie uciążliwe, ale nie musi tak być. Oto parę zasad, których warto się trzymać, by nie dać się oszukać, czy nie wgrać sobie na urządzenie złośliwego oprogramowania.

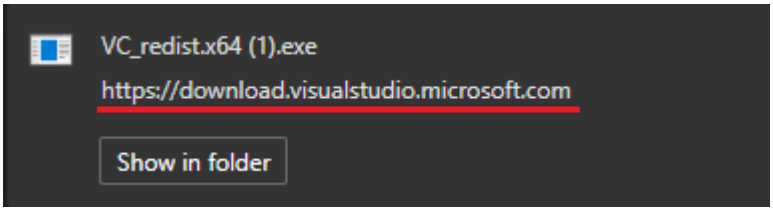
Co dotyczy pobierania plików:

1. **Nie uruchamiaj** programów wysłanych przez innych użytkowników (np. na komunikatorze lub przez e-mail) – bez względu na to czy ufasz takiej osobie czy nie.
   Dlaczego?
   Bardzo często przeprowadzana jest w ten sposób kradzież kont i masowe rozsyłanie złośliwego oprogramowania.
2. Jeśli pobierasz programy z mniej popularnych stron, poszukaj w Internecie **informacji czy są bezpieczne.**
3. Używaj rozszerzeń przeglądarki **blokujących reklamy** (np. uBlock Origin).
4. Jeśli nie chcesz ich używać, przy pobieraniu plików upewnij się, że są pobierane z poprawnego adresu. Warto to robić, ponieważ istnieje wiele reklam, które wyglądają jak np. przycisk pobierania. **Adres serwera**, z którym połączył się komputer możemy znaleźć w historii pobierania przeglądarki.

   Firefox:



   Edge:



O czym jeszcze koniecznie musicie pamiętać?

1. Nie używajcie takich samych haseł w różnych serwisach!
   Gdy zdarzy się wyciek danych z jednego portalu, hakerzy będą mogli się zalogować do **wszystkich serwisów**, do których logujecie się za pomocą tych samych danych.
   Przydatnym narzędziem jest menedżer haseł (np. KeePassXC).
2. Zmieniajcie **ustawienia prywatności** w serwisach, które używacie. Zwykle te domyślne są tak skonstruowane, by zbierały jak najwięcej o was informacji
3. Zawsze weryfikujcie **domenę adresu nadawcy** przy otwieraniu wiadomości e-mail (domena to np. google.com w example@google.com). Sprawdź, czy jest ona zgodna z domeną serwisu, z którego spodziewacie się wiadomości.
4. Jeśli dana oferta wydaje się **za dobra**, by była prawdziwa, to jest to sygnał by się zastanowić, czy przypadkiem nie jest ona oszustwem.

2. Prywatność w sieci: Jak nasze dane są wykorzystywane?

Informacja to potęga. Właśnie dlatego wszystkie organizacje i firmy, którym zależy na rozwoju i zysku próbują zbierać jak najwięcej danych o swoich użytkownikach. Każdy serwis, którego używamy (szczególnie, jeśli za niego nie płacimy) zarabia ze zbierania o nas informacji.

Jakie dane są gromadzone?

Historia wyszukiwania, lokalizacja, informacje demograficzne, zainteresowania, oglądane przez nas treści i o wiele więcej. Pozyskuje się wszystko, co może się przydać do przewidzenia **działań i zainteresowań** użytkownika.

Pewnie zadajecie sobie pytanie: dlaczego ktoś chciałby wiedzieć to wszystko o swoich klientach? Przecież przechowywanie tak ogromnej ilości danych musi sporo kosztować.

Tak, ale jest to nic, w porównaniu z tym, co można nimi zarobić.

Przykładem jest **model biznesowy platform społecznościowych**. Gromadzone są dane o tym, co ludzie robią na platformie – co lajkują, komentują, oglądają – a potem wykorzystywane, aby wyświetlać reklamy dopasowane do ich zainteresowań. Im lepiej reklama trafia w gusta użytkownika, tym większa szansa, że coś kupi, co jest korzystne dla reklamodawców. Jeśli platforma nie ma wystarczająco dużo danych, może je sprzedać firmom reklamowym, które użyją ich do jeszcze lepszego dopasowywania reklam do użytkownika.

Co możemy z tym zrobić?

Niestety, bez radykalnych działań, nie możemy tego całkowicie powstrzymać. Najlepszą strategią jest czytanie **polityki prywatności** każdego serwisu, którego chcemy użyć i decydowanie, czy według nas jest warto jest to robić. Nie dziwne jest, że pewnie w waszej głowie pojawiła się myśl, że to żmudne i czasochłonne zadanie - w 100% się z tym zgadzamy.

Prostszym, lecz mniej efektywnym rozwiązaniem jest dostosowywanie **ustawień prywatności** w używanych przez nas portalach. Chodzi o proste czynności, takie jak wyłączanie Wi-Fi, Bluetooth oraz usług GPS w telefonie, gdy ich nie używamy. Korzystnie jest również używać rozszerzeń blokujących reklamy (np. uBlock Origin) i regularnie usuwać pliki cookie z przeglądarki.

VI
Świadome korzystanie z technologii

1. Etyka sztucznej inteligencji: Jakie są granice?

Zasady etyczne, a używanie sztucznej inteligencji to definitywnie idealne pole do burzliwych dyskusji.

Najwięcej kontrowersji wzbudza przede wszystkim **generatywna sztuczna inteligencja,** czyli taka zajmująca się tworzeniem tekstu, zdjęć, obrazów lub filmów. Pewnie zauważyliście, że w sieci pojawia się coraz więcej treści, które nie mają prawie żadnego wkładu ludzkiego.

Dlaczego ten temat wzbudza takie emocje?

Jest kilka odpowiedzi na to pytanie, spójrzmy na te najbardziej oczywiste. Jesteśmy przekonani, że wiecie, że twórcy Internetowi i artyści muszą wkładać bardzo dużo pracy, w każdy swój projekt. Często nadużywanie AI może zostać **odebrane jako oszukiwanie**, a w ten sposób powstałe materiały zazwyczaj są znacznie gorszej jakości. Sztucznej inteligencji brakuje ludzkich uczuć, przez co pisanym przez nią treści brakuje kreatywności i głębi (np. w scenariuszach), a na dodatek większość z nich posiada prawie identyczną strukturę, przez co są przewidywalne.

Poważniejszym problemem jest fakt, że modele AI muszą być na czymś **trenowane**. To znaczy, że potrzebna jest niewyobrażalna ilość przykładów, by mogła się uczyć. Skutkuje to masowym używaniem prac różnego rodzaju twórców bez ich zgody. Co was pewnie nie zdziwi - wielu artystów nie życzy sobie by ich twórczość posłużyła temu celowi.

Taki zabieg może doprowadzić do podobieństwa generowanych treści przez AI do dzieł danego twórcy. Odbiorcy wtedy mogą pomyśleć, że ten oryginalny artysta wykorzystał sztuczną inteligencję w bardzo dużym stopniu, a w rzeczywistości mógł nawet nie zdawać sobie sprawy, że jego prace zostały w tym celu wykorzystane.

Musicie także pamiętać, że modele AI mogą być poddane **cenzurze**, czy **manipulacji**. Firma, która udostępnia nam swój może modyfikować jego odpowiedzi, jak tylko jej się podoba.

Przykładem na to jest model Deepseek, który nie odpowie na tematy niewygodne dla chińskiej partii komunistycznej. Wniosek jest jeden - zawsze trzeba weryfikować wszystkie informacje, które otrzymamy z takiego typu systemów.

2. Dobra, a co dalej? - przyszłość cyberbezpieczeństwa i sztucznej inteligencji

Podczas gdy rozwijają się nowe technologie, strefa cyberbezpieczeństwa nieustannie ulega zmianom.

Dzieje się tak, ponieważ coraz więcej korzystamy z usług w chmurze, które zyskują cały czas na popularności. Każda nowinka technologiczna wiąże się z nowymi potencjalnymi lukami w bezpieczeństwie, które mogą być wykorzystane przez hakerów.

Z tego powodu nieustannie prowadzone są prace nad rozwiązaniami zwiększającymi bezpieczeństwo. Przykładem jest model **Zero Trust**, który zakłada brak domyślnego zaufania wobec urządzeń w sieci – dopóki ich użytkownicy nie zostaną zweryfikowani. Dodatkowo systemy otrzymują jedynie minimalne uprawnienia niezbędne do wykonania swoich zadań. Ważnym założeniem tego modelu jest świadomość, że **ataki i wycieki danych są nieuniknione**, dlatego należy przewidywać najgorsze scenariusze i odpowiednio się na nie przygotować.

Czy wiedzieliście, że rozwój sprzętu komputerowego znacząco zwolnił? Może to być zaskakujące, ale coraz trudniej jest projektować i produkować **bardziej wydajne procesory**, które będą działać szybciej i sprawniej niż dotychczasowe.

Następnym krokiem w ewolucji technologii są **komputery kwantowe**.

Ich sposób działania różni się od tradycyjnych komputerów, co sprawia, że obecnie stosowane metody szyfrowania danych stają się wobec nich nieskuteczne. W związku z tym istnieje konieczność opracowania algorytmów szyfrowania odpornych zarówno na ataki klasycznych komputerów, jak i tych kwantowych.

Sztuczna inteligencja również może odegrać kluczową rolę w cyberbezpieczeństwie przyszłości. Może zostać wykorzystana do wykrywania nietypowego ruchu sieciowego, identyfikacji złośliwego oprogramowania i ochrony urządzeń przed cyberatakami.

Niestety, AI może być także narzędziem w rękach cyberprzestępców – do pomocy w uzyskaniu nieautoryzowanego dostępu do systemu, czy pisania złośliwego oprogramowania lub automatyzacji ataków. To wyśmienite narzędzie do analizy danych (np. formatowanie i grupowanie skradzionych informacji).

Nowe technologie, jak widać, mogą być wykorzystywane w różnych celach – zarówno w służbie bezpieczeństwa, jak i w rękach osób o złych intencjach. Dlatego kluczowe jest nie tylko ich rozwijanie, ale także odpowiedzialne i świadome ich używanie.

Zakończenie

Dziękujemy, że poświęciliście czas na zapoznanie się z naszym materiałem.

Mamy nadzieję, że wiedza, którą zawarliśmy w tym e-booku okazała się intrygująca i zachęciła was do dalszej eksploracji świata cyberbezpieczeństwa i sztucznej inteligencji.

W dynamicznie zmieniającym się świecie technologii kluczowe jest, abyśmy byli świadomi zagrożeń i potrafili odpowiednio się przed nimi zabezpieczyć. Taki jest nasz cel - chcemy by coraz więcej ludzi o tym wiedziało.

Dlatego powstał nasz projekt. Działamy w ramach olimpiady “Zwolnieni z teorii” i pilnie potrzebujemy waszego wsparcia w jego realizacji. Żeby nie było - już to zrobiliście zagłębiając się w naszą pracę, ale niezmiernie miło nam będzie jak wesprzecie nas także w mediach społecznościowych.

Nic was to nie kosztuje, a nam daje ogromne możliwości dalszego rozwoju.

Linki do naszych social mediów:

Instagram: https://www.instagram.com/cyberaware.pl/

Facebook: https://www.facebook.com/profile.php?id=61568076243423

Nasze podcasty: https://open.spotify.com/show/3sh5Bn5DvaxKgYBj1hZcq8?si=1a87882ae5534caf&nd=1&dlsi=fdd81495700d4bf5

Do następnego,

Zespół CyberAware