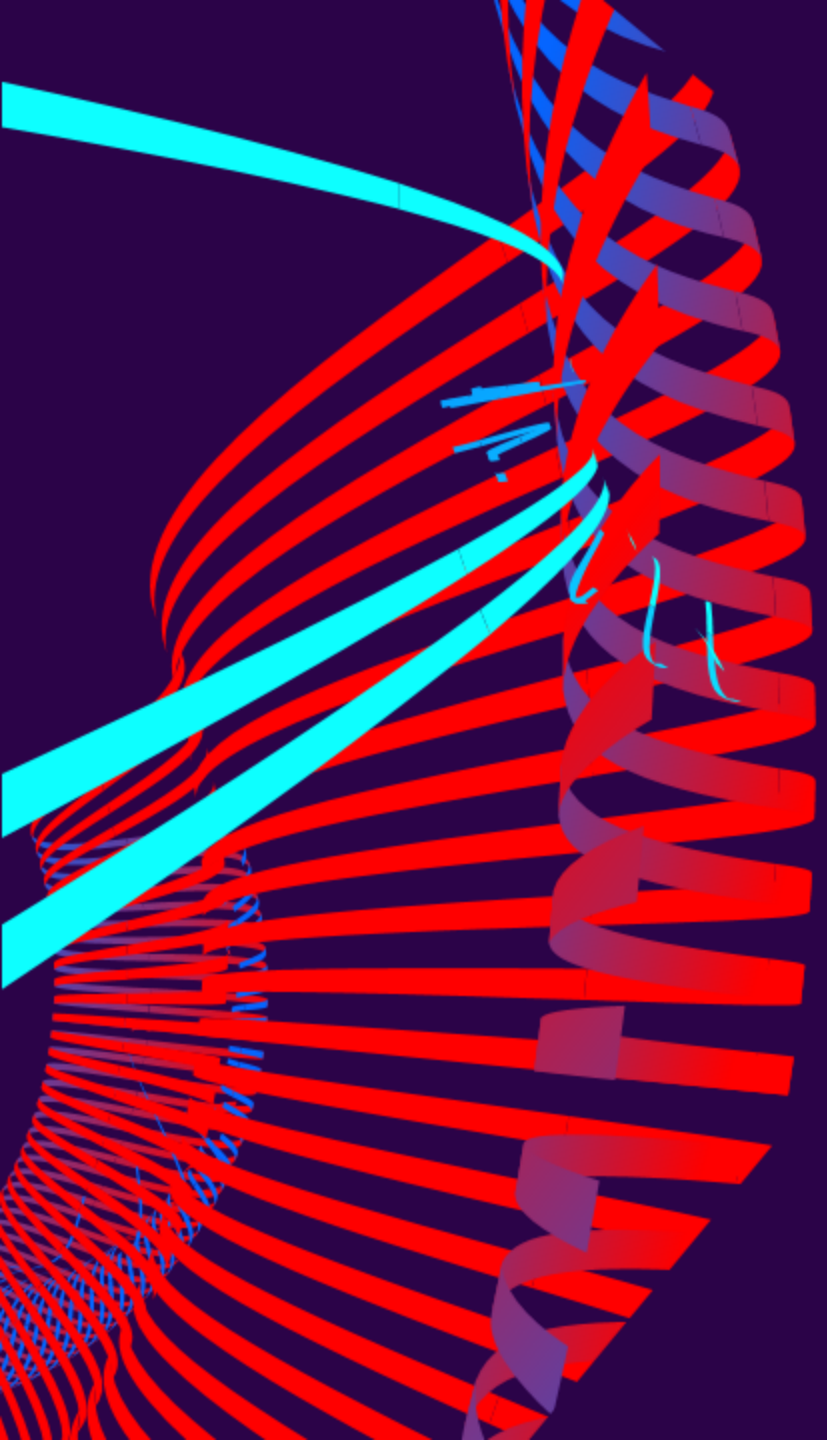
ZASADY CYBERBEZPIECZEŃSTWA

Brajan Miastkowski

Kamil Ziemianin

DEFINICJA CYBERBEZPIECZEŃSTWA

Cyberbezpieczeństwo odnosi się do praktyk, technologii i procesów zaprojektowanych do ochrony systemów komputerowych, sieci, danych i informacji przed nieautoryzowanym dostępem, zmianami lub zniszczeniem. Jest to kompleksowy zestaw działań mających na celu zapobieganie atakom cybernetycznym oraz minimalizowanie szkód w przypadku ich wystąpienia.



SKUTKI NIE PRZESTRZEGANIA ZASAD CYBERBEZPIECZEŃSTWA

SKUTKI NIE PRZESTRZEGANIA ZASAD

Kradzież tożsamości

Może to prowadzić do użycia czyjejś tożsamości do dokonywania oszustw finansowych, otwierania fałszywych kont lub uzyskiwania kredytów na czyjeś nazwisko.

Utrata danych osobowych

Może prowadzić do wycieku takich jak numery kart kredytowych, hasła czy adresy e-mail.

Straty finansowe

Mogą obejmować utratę pieniędzy z konta bankowego, lub konieczność poniesienia dodatkowych kosztów związanych z naprawą skutków ataku.

Wirusy i malware

Użytkownik może być narażony na zainfekowanie swojego komputera przez wirusy, trojany lub inne złośliwe oprogramowanie, co prowadzi do utraty kontroli nad urządzeniem, kradzieży danych.

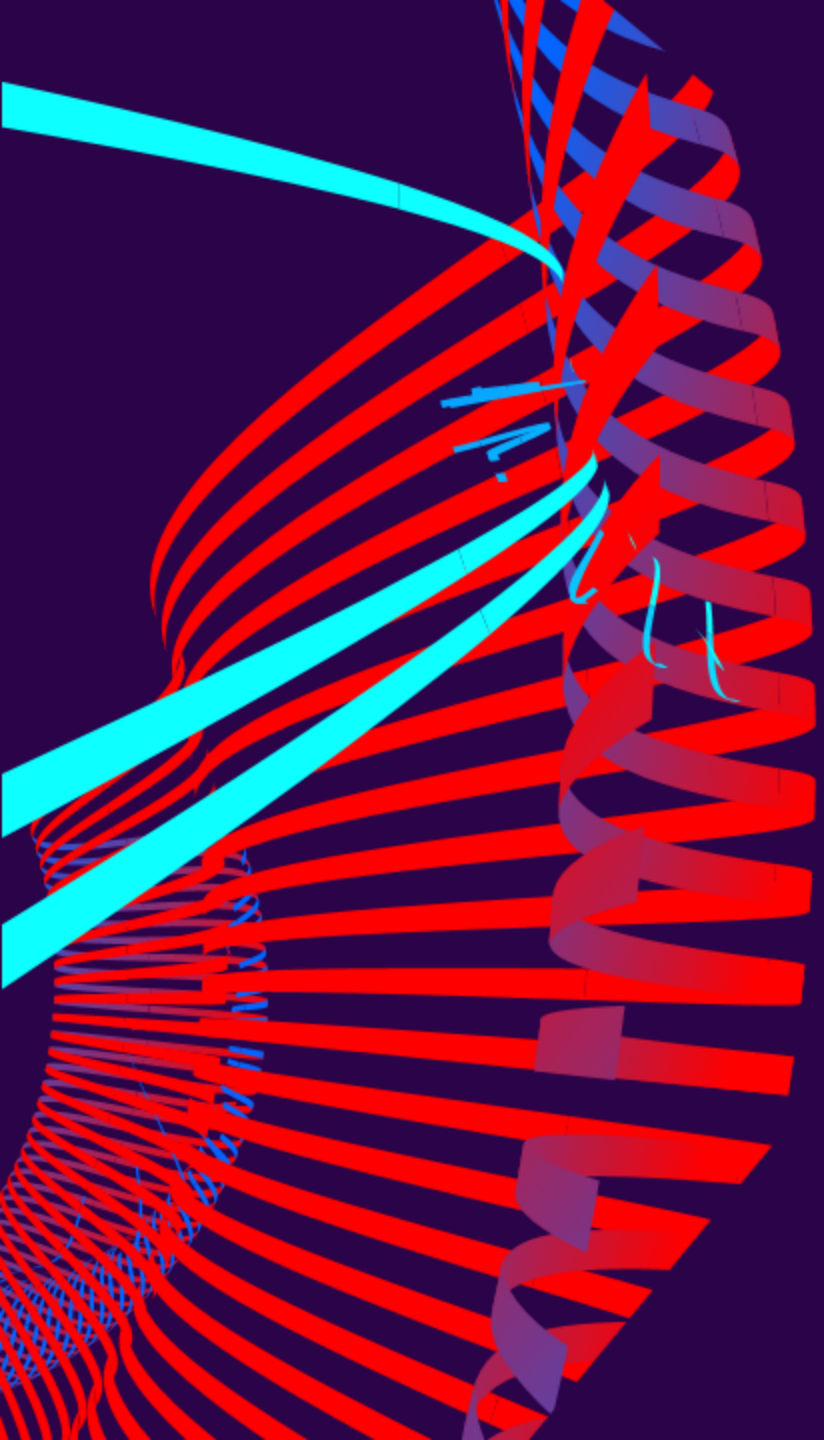
SKUTKI NIE PRZESTRZEGANIA ZASAD

Używanie urządzenia do ataków

Urządzenie może być wykorzystane przez cyberprzestępców do przeprowadzenia ataków na inne systemy lub sieci. Użytkownik może nie zdawać sobie sprawy z tego, że jego urządzenie jest wykorzystywane do szkodliwych działań.

Naruszenie prywatności

Cyberprzestępcy mogą zdalnie przejąć kontrolę nad kamerą lub mikrofonem urządzenia, co pozwoli im na podsłuchiwanie użytkownika lub nagrywanie prywatnych rozmów i działań.



ZASADY CYBERBEZPIECZEŃSTWA

ZASADY CYBERBEZPIECZEŃSTWA

Sens świadomości

Zrozumienie zagrożeń w sieci oraz świadomość konsekwencji niewłaściwego korzystania z technologii. Edukacja w tym zakresie jest kluczowa.

Silne hasła

Używaj unikalnych, silnych haseł dla każdego konta online. Hasła powinny zawierać kombinację dużych i małych liter, cyfr oraz znaków specjalnych, a także być regularnie zmieniane.

Aktualizacje oprogramowania

Regularne aktualizacje oprogramowania, w tym systemu operacyjnego, przeglądarki i aplikacji, by ubezpieczyć się przed lukami w zabezpieczeniach.

Używanie oprogramowania antywirusowego i zaporowego

Instalacja oprogramowania antywirusowego i zaporowego pomaga w identyfikacji i blokowaniu złośliwego oprogramowania oraz ataków sieciowych.

ZASADY CYBERBEZPIECZEŃSTWA

Szyfrowanie danych

Korzystaj z usług, które oferują szyfrowanie danych, szczególnie gdy przekazujesz wrażliwe informacje przez internet, takie jak hasła czy dane finansowe.

Regularne kopie zapasowe

Regularne tworzenie kopii zapasowych danych jest niezwykle istotne w przypadku ataku ransomware lub utraty danych z innych przyczyn.

Uważność na phishing

Bądź ostrożny w przypadku podejrzanych wiadomości e-mail, SMS-ów czy telefonów. Phishing to metoda ataku, w której cyberprzestępcy podszywają się pod zaufane instytucje w celu wyłudzenia poufnych informacji.

PODSUMOWANIE

Cyberbezpieczeństwo jest kluczowym elementem naszej obecności w cyfrowym świecie. Wdrażanie zasad cyberbezpieczeństwa nie tylko chroni nasze dane osobowe i biznesowe, ale również pomaga w ochronie całego społeczeństwa przed cyberzagrożeniami.

DZIĘKUJEMY

Brajan Miastkowski

Kamil Ziemianin