

Wydział Prewencji Zagrożeń CAT ABW

<https://www.tpcoe.gov.pl/cpt/materialy/1841,Cyberbezpieczenstwo.html>
03.05.2025, 13:14

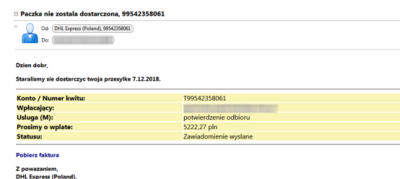
Cyberbezpieczeństwo

Dynamiczny rozwój Internetu i nowych technologii stworzył wiele możliwości i udogodnień, ale również zagrożeń. Internet stał się groźnym narzędziem w rękach terrorystów i przestępców, którzy wykorzystują go do swoich celów. Odpowiedzialne korzystanie z usług internetowych oraz nowoczesnych urządzeń pozwala uniknąć większości zagrożeń w cyberprzestrzeni.

ABW rekomenduje stosowanie się do opisanych poniżej zaleceń, które stanowią wybrane elementy tzw. higieny pracy w Internecie, czyli bezpiecznego korzystania z sieci.

Propaganda terrorystyczna

Nie udostępniaj i nie przekazuj dalej treści terrorystycznych w Internecie, gdyż leży to w interesie terrorystów. Takie działania mogą przyczynić się do podejmowania prób naśladowania poczynąń terrorystów



Przykład podejrzanej wiadomości zawierającej złośliwy załącznik. Nie pobieraj tego rodzaju załączników i nie klikaj w linki przesłane przez nieznanym/podejrzanych nadawców!



przez osoby podatne na radykalizację lub niestabilne psychicznie.

Zobacz film o propagandzie terrorystycznej

online: [https://www.youtube.com/watch?v=fun_sRDxdu](https://www.youtube.com/watch?v=fun_sRDxduQ)

[Q](https://www.youtube.com/watch?v=fun_sRDxduQ)

Próby werbunku

Upewnij się, że Twoje dzieci w bezpieczny sposób korzystają z Internetu, ponieważ są one najłatwiejszym celem dla terrorystów. Osoby młode, podatne na radykalizację lub przejawiające skłonność do agresji, mogą być zachęcane do wstąpienia do różnego rodzaju organizacji terrorystycznych.

Wykradanie danych

Pamiętaj o tym, że wszystkie dane, które znajdują się w Internecie, są również widoczne dla terrorystów. Dane o Twoich kontaktach i miejscu pracy mogą zostać użyte na etapie planowania zamachu terrorystycznego. Nie udostępniaj na portalach społecznościowych informacji, które mogłyby zostać wykorzystane przez terrorystów lub przestępców.

Tworzenie haseł

Twórz silne hasła – powinny się one składać z małych i wielkich liter, cyfr i znaków specjalnych. Nie używaj jednego hasła do wszystkich usług (np. skrzynka pocztowa, bank, portal społecznościowy). Co jakiś czas staraj się zmieniać hasła na nowe.

Pobieranie plików z Internetu

Nie pobieraj żadnych plików z Internetu, co do których

pochodzenia nie masz absolutnej pewności. Nie otwieraj żadnych załączników e-maili, chyba że są one oczekiwane i pochodzą od znanych nadawców. Wszystkie załączniki przeskanuj aktualnym programem antywirusowym.

Zgłaszanie incydentów

Wszystkie podejrzane wiadomości zgłaszaj niezwłocznie osobie odpowiedzialnej w Twoim miejscu pracy za bezpieczeństwo teleinformatyczne. W przypadku braku takiej możliwości pamiętaj, że wszystkie incydenty teleinformatyczne w urzędzie lub instytucji państwowej możesz zgłosić również na stronie: www.csirt.gov.pl.

Zapraszamy do zapoznania się z przygotowanymi przez ABW animacjami dotyczącymi cyberbezpieczeństwa, które dostępne są na kanale YouTube 4U:

- <https://www.youtube.com/watch?v=IEeJMLbCPMA>
- <https://www.youtube.com/watch?v=v9qN7rDrQ1c>
- <https://www.youtube.com/watch?v=gdMzOuhz2qU>
- <https://www.youtube.com/watch?v=BrhRc2hcB6I>
- https://www.youtube.com/watch?v=XZCZte_6bR4
- https://www.youtube.com/watch?v=PDcLx-L1_AA
- https://www.youtube.com/watch?v=CuYLSXF_G8pl

Zachęcamy również do zapoznania się z materiałami dot. cyberbezpieczeństwa, dostępnymi w serwisie gov.pl pod adresem: <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo>

Kurs e-learningowy

Cyberbezpieczeństwo stanowi jeden z pięciu modułów kursu e-learningowego z zakresu prewencji terrorystycznej, który CAT ABW prowadzi za pośrednictwem

portalu: <https://learning.tpcoe.gov.pl/> Kurs

dedykowany jest dla funkcjonariuszy służb oraz pracowników administracji publicznej. Więcej informacji znajdziesz pod

adresem: <https://tpcoe.gov.pl/cpt/wydarzenia/1807,CP-T-ABW-otwiera-portal-e-learningowy.html>

[Poprzedni Strona](#)
[Następny Strona](#)