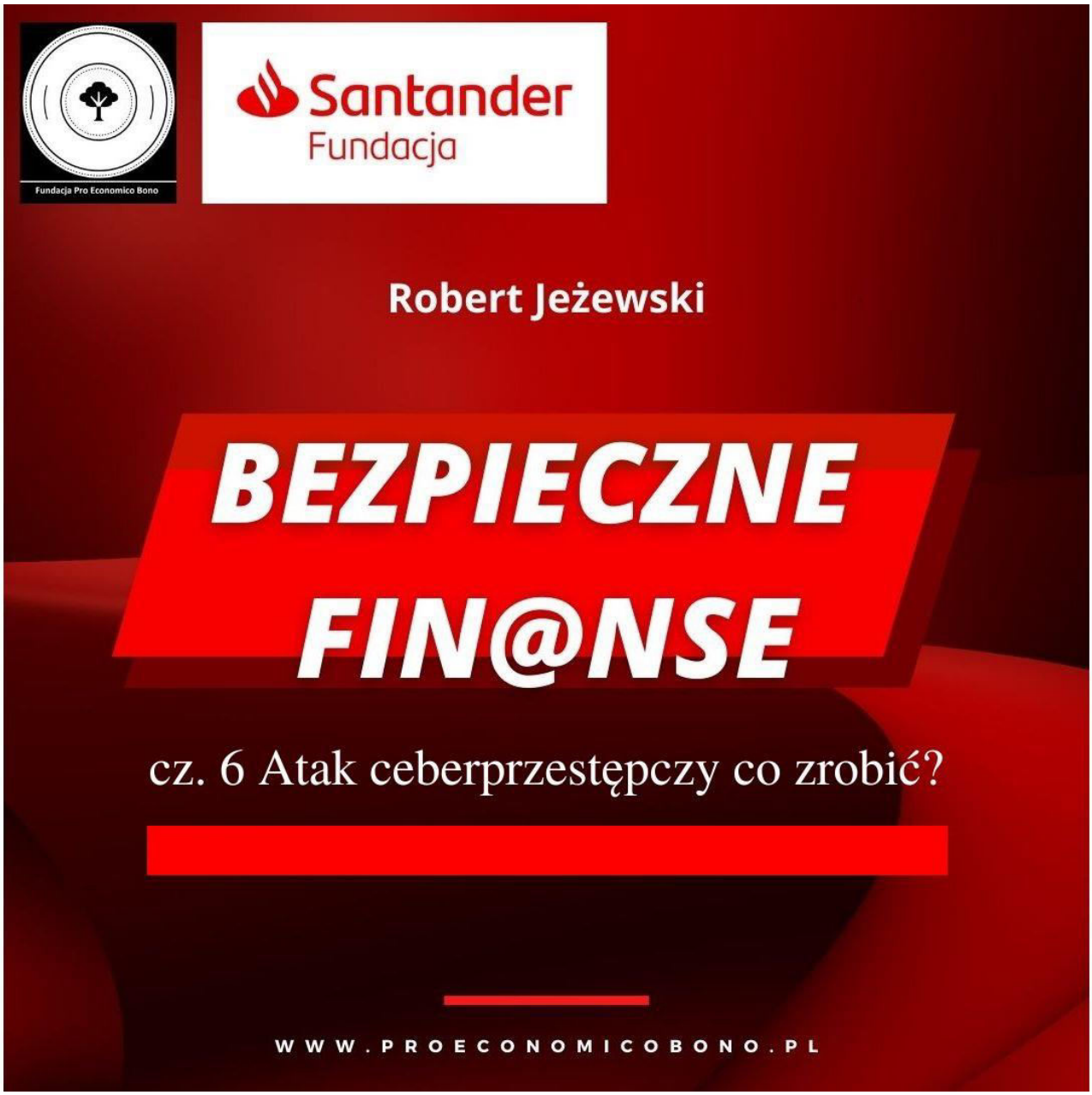


Haki na cyberataki

Bezpieczne Fin@nse

cz. 6 Atak cyberprzestępczy co zrobić?

Słowo wstępu

Starzenie się społeczeństwa jest obecnie procesem uznawanym za powszechny trend w krajach Europy Zachodniej. Społeczne transformacje przynoszą jakościowe zmiany w sposobie definiowania wykluczenia społecznego. Konsekwencje starzenia się społeczeństwa niosą wiele obaw o przyszłość krajów europejskich, w tym także Polski.

Współczesna rzeczywistość ulega szybkim przeobrażeniom w wielu obszarach. Umiejętność przystosowywania się do zachodzących zmian nabiera cywilizacyjnego wymiaru. Na szczególną uwagę zasługuje gwałtowny postęp technologiczny i rozwój rynku nowych technologii, zwłaszcza informacyjno-komunikacyjnych. Współczesne systemy społeczno gospodarcze społeczeństwa, a także państwa są uzależnione od technologii.

Umiejętność bezpiecznego korzystania z nowych technologii informacyjno-komunikacyjnych staje się koniecznością, a jej brak skutkuje ostracyzmem , społecznym wykluczeniem, narażeniem na ataki, które kończą się utratą środków. Internet a także rozwój aplikacji jest najtrudniejszy do zaakceptowania i czynnego używania jest przez seniorów. Wynika to z mniejszego tempa przyswajania wiedzy, ale też ostracyzmu tej grupy społecznej. Senior to tak ze łatwy punkt ataku.

Całość składa się z 6 cykli, które zostaną finalnie opublikowane jako jeden podręcznik pt. Bezpieczne Fin@nse. Kolejne części będą się pojawiały w odstępie 3 tygodni, wraz z filmem wprowadzającym do zagadnienia, które będą dostępne m.in. na stronie fundacji Pro Economico Bono, oraz jej mediach społecznościowych (Facebook, You Tube).

1) Bezpieczne korzystanie z e-bankowości
2) Bezpieczne korzystanie z m-bankowości
3) Bezpieczne korzystanie z karty kredytowej i debetowej (płatności w sklepie i wypłata z bankomatu)
4) Bezpieczne korzystanie z social media (komunikatory What's App podawanie danych newralgicznych)
5) Bezpieczne korzystanie z płatności za zakupy w Internecie
6) Atak ceberprzestępczy co zrobić?

Dzięki poradnikowi osoby starsze:

1. zwiększą wiarę w otworzenie i własne możliwości związane z bezpiecznym
2. korzystaniem z nowych technologii
3. zwiększą samoocenę w aspekcie technologiczno-komunikacyjnym
4. zwiększą motywację do bezpiecznego korzystania z nowych technologii, a zarazem oszczędności czasu
5. zmienią sposób myślenia w temacie nowych technologii i bezpieczeństwa z nimi związanych

Obecnie oddaję Państwu do czytania cz. 6 Poradnika Bezpieczne Fin@nse
Atak cyberprzestępczy co zrobić?

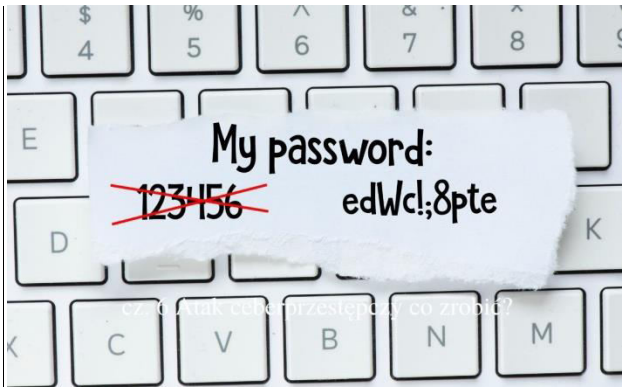
Zapraszam do lektury i zgłębiania tematu, jakże ważnego w dzisiejszym, bardzo dynamicznym otoczeniu.

prof. ucz. dr inż. Robert Jeżewski

Prezes Zarządu Fundacji Pro Economico Bono

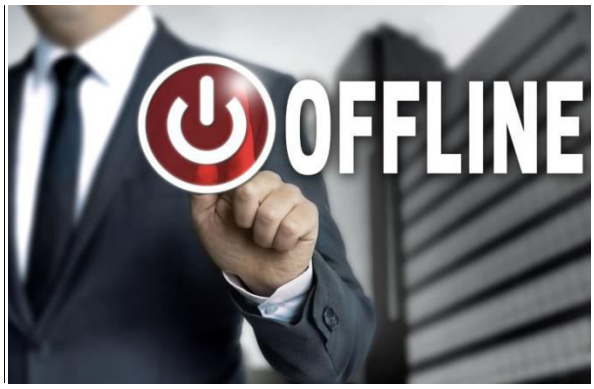
cz. 6 Atak cyberprzestępczy co zrobić?

1. **ZMIEŃ HASŁO**



Zmień hasło zgodnie z zasadą używania małych i dużych liter, oraz znaków specjalnych. Zmiana hasła dotyczy miejsca, gdzie miał atak cyberprzestępczy tj. konto bankowe, konto social media, itp.

2. **ODETNIJ SIĘ OD SIECI (BĄDŹ OFFLINE)**

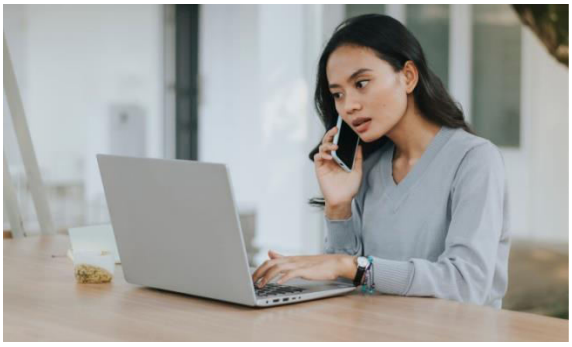


Odetnij się od sieci (bądź offline). Działanie ma na celu odcięcie cyberprzestępcy od zdalnego zarządzania Twoim komputerem.

3. **PRZESKANUJ KOMPUTER ZA POMOCĄ PROGRAMU ANTYWIRUSOWEGO**

Przeskanuj komputer za pomocą programu antywirusowego (programu antywirusowego offline). Program antywirusowy będzie poszukiwał anomalii w Twoim komputerze i po znalezieniu złośliwego oprogramowania, podda je kwarantannie i/lub usunie.

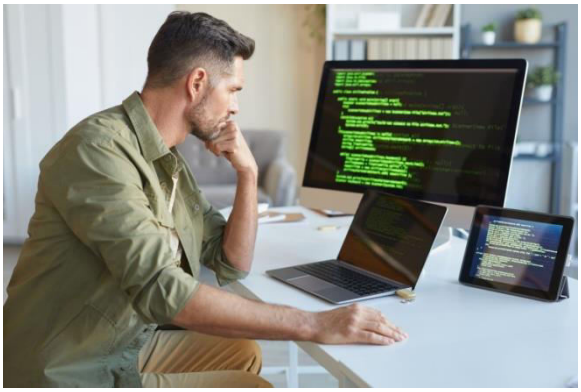
4. ZGŁOŚ INCYDENT DO ODPOWIEDNICH SŁUŻB



Koniecznie zgłoś incydent na infolinię banku lub bezpośrednio w placówce banku. Pracownik szczegółowo poinformuje cię, jak wygląda procedura i dalsza ścieżka realizacji zgłoszenia. W szczególnych przypadkach konieczna może okazać się blokada karty płatniczej, eskalacja zdarzenia i złożenie doniesienia o popełnionym przestępstwie na policję. Dlatego ważna jest tutaj współpraca i nie ukrywanie faktów dot. zdarzenia.

W przypadku włamania do konta na social media, koniecznie zgłoś incydent do centrum wsparcia użytkownika. Nie bagatelizuj sytuacji. Te dane mogą posłużyć dalej cyberprzestępcy do wyłudzenia danych bankowych i wyłudzania pieniędzy od Twoich znajomych.

5. JEŚLI PROGRAM ANTYWIRUSOWY NIE POMAGA, KONIECZNIE ZAINSTALUJ SYSTEM OD NOWA



Jeśli program antywirusowy nie jest w stanie sobie poradzić ze złośliwym oprogramowaniem, konieczne będzie wykonanie twardego formatowania dysku i zainstalowanie całego oprogramowania od nowa.

Literatura:

1. Anderson R., Inżynieria zabezpieczeń, Wydawnictwa Naukowo-Techniczne, Warszawa 2005
2. Cole E., Krutz R. L., Conley J., Bezpieczeństwo sieci - Biblia, Wydawnictwo HELION, Gliwice 2005
3. Gibson,W., Neuromancer. Katowice: Wydawnictwo Książnica 2009
4. Kontselidze A., Cyberterrorism – when technology became a weapon, „European Scientific Journal" 2015
5. Negroponte J. D., Palmisano S.J., Segal A., Defending an Open, Global, Secure, and Resilient Internet, Nowy Jork 2013
6. Nowakowski, Z., Szafran H., Szafran R., Bezpieczeństwo w XXI wieku. Strategie bezpieczeństwa narodowego Polski i wybranych państw. Rzeszów: Politechnika Rzeszowska 2009
7. Strebe M., Bezpieczeństwo sieci - podstawy, Wydawnictwo MIKOM, Warszawa 2005
8. Webster W., Cilluffo F., Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo, Waszyngton 1998