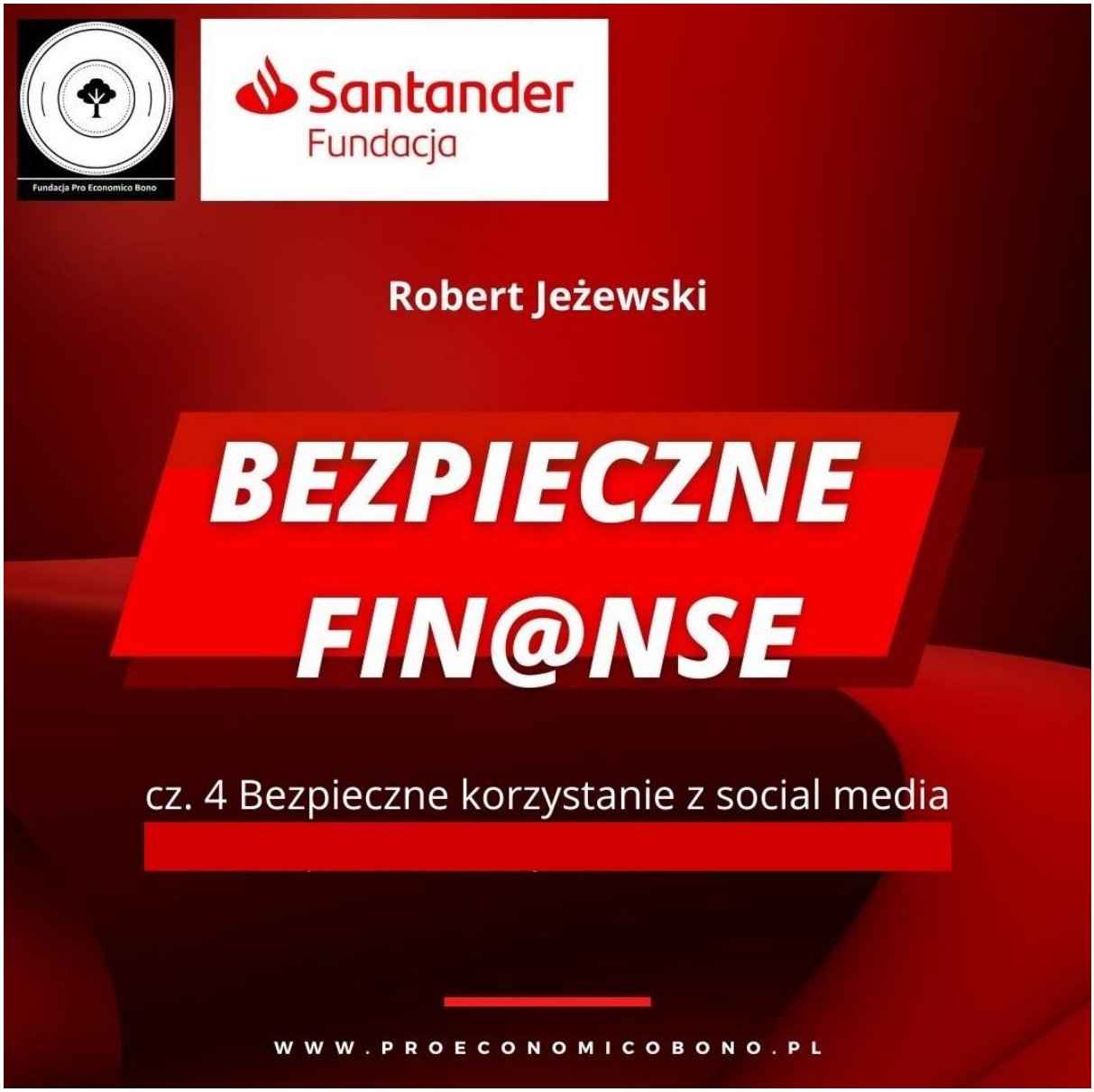


Haki na cyberataki

Bezpieczne Fin@nse

cz. 4 Bezpieczne korzystanie z social media

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. 4 Poradnika Bezpieczne Fin@nse Bezpieczne korzystanie z social media.

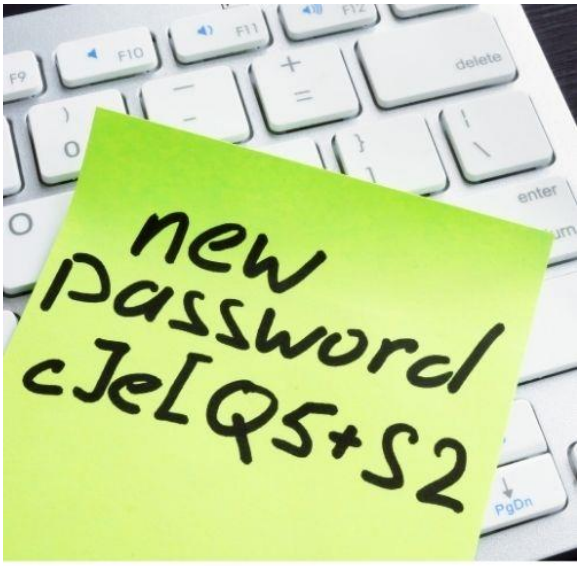
Zapraszam do lektury i zgłębiania tematu, jakże ważnego w dzisiejszym, bardzo dynamicznym otoczeniu.

prof. ucz. dr inż. Robert Jeżewski

Prezes Zarządu Fundacji Pro Economico Bono

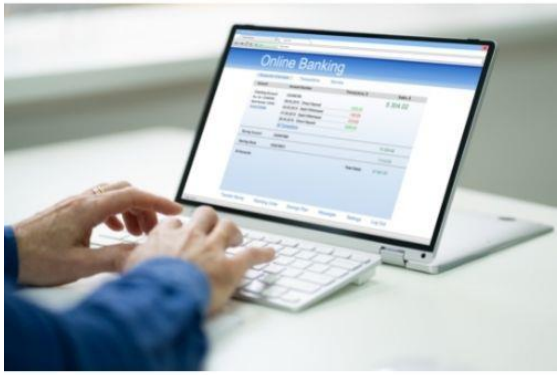
cz. 4 Bezpieczne korzystanie z social media

1. ZAWSZE TWÓRZ SILNE HASŁO



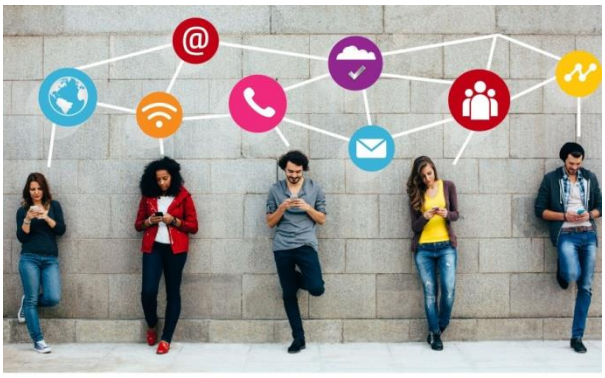
Konto w serwisie społecznościowym ZAWSZE zabezpieczaj indywidualnym i odpowiednio długim hasłem. Wielu użytkowników korzysta ZAWSZE z tego samego hasła do wielu kont. To bardzo zły nawyk. Każde hasło powinno być nie tylko silne, ale też indywidualne do każdego konta. To zniechęci cyberprzestępców i uchroni Twoje dane.

2. OGRANICZ DOSTĘP DO SWOJEGO KONTA POPRZEZ DWUSTOPNIOWE UWIERZYTELNIANIE



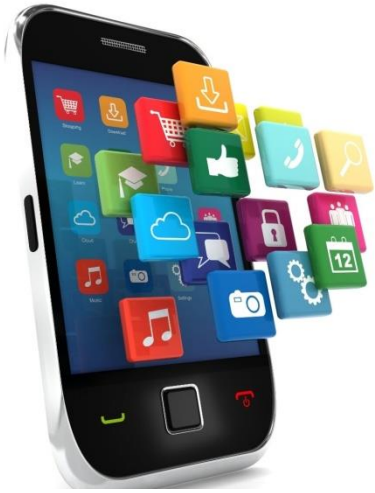
Aktywuj dwustopniowe uwierzytelnianie na wszystkich swoich kontach w mediach społecznościowych. Można z niego korzystać w większości serwisów social media. To dodatkowy etap ochrony, który zabezpieczy Twoje dane.

3. DODAWAJ TYLKO PRAWDZIWYCH ZNAJOMYCH



Dodawaj do listy znajomych TYLKO osoby, które rzeczywiście znasz i którym ufasz. Pamiętaj, że przyjmując nową osobę (osobę nieznaną) do grupy swoich znajomych, najczęściej domyślnie udostępniasz jej informacje o sobie, oraz swoje zdjęcia.

4. KORZYSTAJ TYLKO Z OFICJALNYCH APLIKACJI SIECI SPOŁECZNOŚCIOWYCH

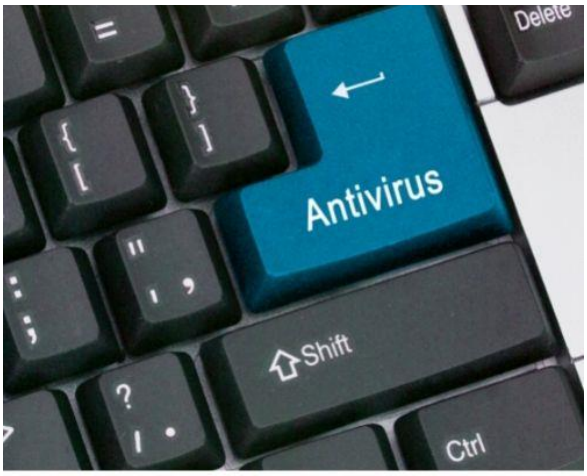


Aplikacje pobieraj TYLKO z oficjalnych sklepów tj. Google Play dla Android, App Store dla Ios, oraz Microsoft Store dla Windows.

5. DBAJ O SWOJĄ PRYWATNOŚĆ

Praktycznie wszystkie serwisy społecznościowe posiadają rozwiązania zwiększające prywatność – ZAWSZE je aktywuj.

6. ZAWSZE UŻYWAJ PROGRAMU ANTYWIRUSOWEGO



Dobry program antywirusowy zatrzyma złośliwe oprogramowanie, zanim jeszcze zostanie ono pobrane na dysk. Najpopularniejsze przeglądarki internetowe ostrzegają o podejrzanych stronach internetowych, dlatego ZAWSZE poważnie traktuj takie ostrzeżenia i NIGDY nie odwiedzaj podejrzanych stron. Mogą one zawierać złośliwe oprogramowanie, które umożliwi przestępcom przejęcie kontroli nad Twoim urządzeniem i dostęp do Twoich danych.

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