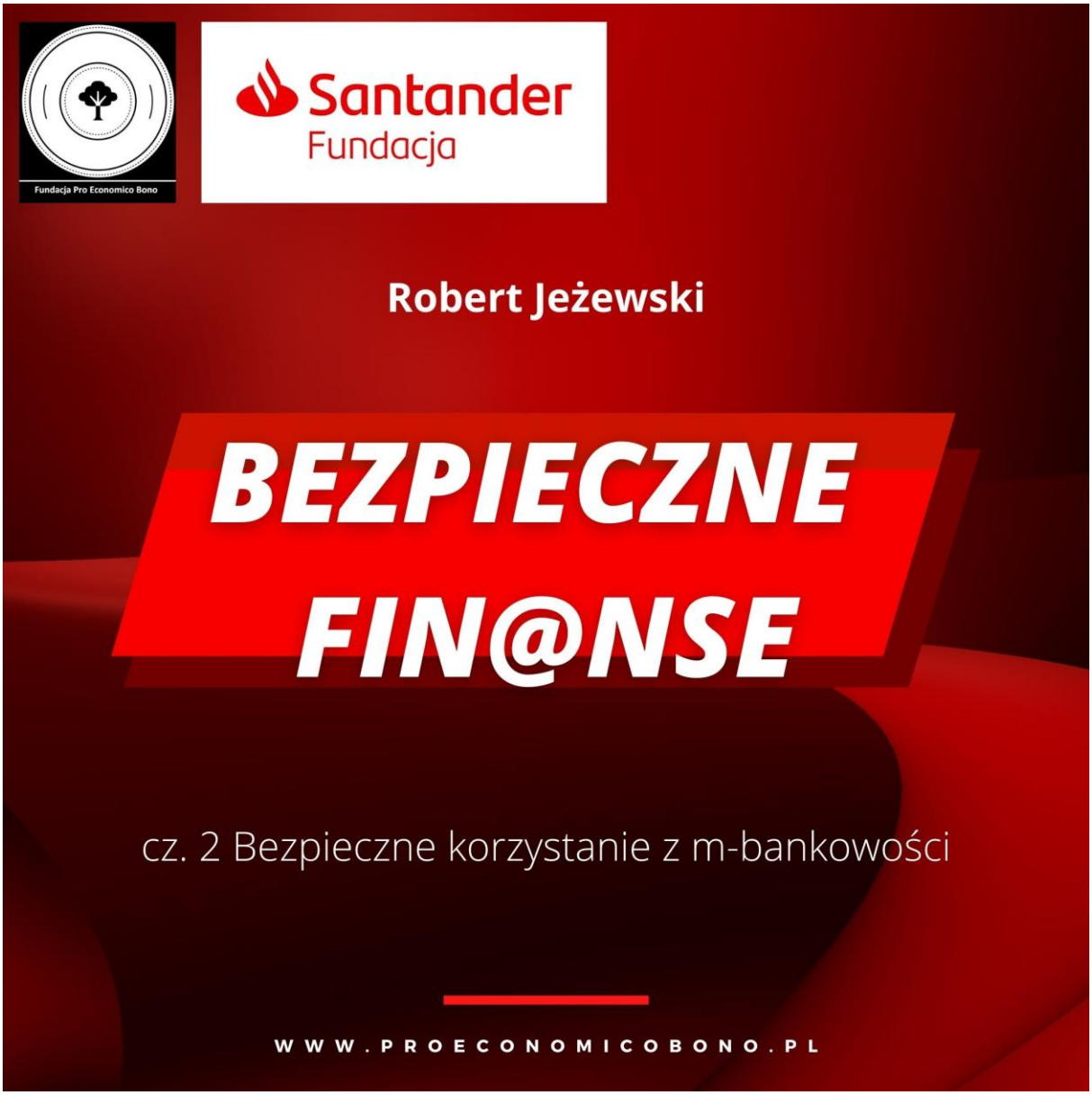


Haki na cyberataki

Bezpieczne Fin@nse

cz. 2 Bezpieczne korzystanie z m-bankowości

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. 2 Poradnika Bezpieczne Fin@nse Bezpieczne korzystanie z m-bankowości.

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. 2 Bezpieczne korzystanie z m-bankowości

1. **ZAWSZE SPRAWDZAJ OD KOGO DOSTAJESZ SMS-A LUB E-MAIL I NIGDY NIE KLIKAJ W LINK, KTÓRY JEST TAM PODANY I PRZEKIEROWUJE CIĘ NA STRONĘ BANKU**

ZAWSZE sprawdzaj od kogo dostajesz SMS-y, lub E_MAIL-e. Bank nigdy nie prosi o logowanie się na rachunek za pomocą linków, wysyłanych w wiadomościach SMS i E-MAIL. Tak działa phishing, czyli technika na podstawie której, cyberprzestępcy podają się za bank i próbują wyłudzić dane do logowania. Strony do logowania wyglądają bardzo podobnie do stron bankowych.

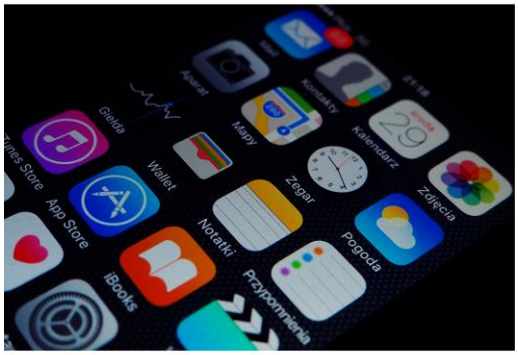
2. **ZAWSZE SPRAWDZAJ CZY STRONA POSIADA WAŻNY PROTOKÓŁ HTTPS**

Protokół HTTPS gwarantuje prywatność i bezpieczeństwo połączenia. Można go sprawdzić najeżdżając kursorem na kłódkę. Kłódka musi być zamknięta a po kliknięciu w nią można sprawdzić, czy certyfikat SSL jest ważny a także na kogo został wystawiony. Jeżeli kłódka jest otwarta i/lub certyfikat wystawiony nie na bank, ZREZYGNUJ z logowania się.

3. **REGULARNIE ZMIENIAJ HASŁO DO LOGOWANIA**

Zmieniaj hasło regularnie, przynajmniej raz w miesiącu. Pozwoli to uniknąć jego deszyfracji za pomocą programów szpiegujących. Dodatkowo ZAWSZE ustalaj hasło, które jest odpowiednio trudne do odgadnięcia. Używaj dużych i małych liter, cyfr, oraz znaków specjalnych tj. @, &, #, $.

4. SPRAWDZAJ BEZPIECZEŃSTWO INSTALOWANYCH APLIKACJI



ZAWSZE sprawdzaj instalowane aplikacje pod kątem ewentualnego zarażenia przez złośliwe oprogramowanie. Instaluj aplikacje TYLKO z pewnego źródła np. sklepów Google Play, czy App Store.

5. NIGDY NIE LOGUJ SIĘ DO BANKOWOSCI MOBILNEJ PRZEZ PUBLICZNĄ SIEĆ WI-FI

NIGDY nie loguj się za pomocą publicznej sieci Wi-Fi. Rodzi to możliwość nadużyć i ingerencji w Twoje urządzenie mobilne ze strony właściciela sieci bezprzewodowej, oraz użytkowników, którzy z niej korzystają.

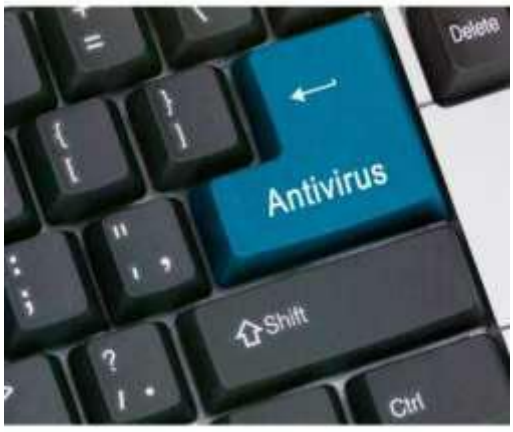
6. **NIGDY NIE LOGUJ SIĘ DO SWOJEJ BANKOWOŚCI ZA POMOCĄ URZĄDZEŃ MOBILNYCH INNYCH NIŻ TWOJE**

Korzystanie z bankowości mobilnej powinno się odbywać TYLKO z Twojego urządzenia mobilnego (smartfon, tablet). Każde inne urządzenie może być zainfekowane złośliwym oprogramowanie, które przechwyci dane do logowania na Twoje konto.

7. **JEŻELI TWOJE URZĄDZENIE NA TO POZWALA STOSUJ ZABEZPIECZENIA BIOMETRYCZNE**

Rozwój technologii upowszechnił wprowadzenie nowego rodzaju zabezpieczeń, jakim są zabezpieczenia biometryczne. Aplikacje bankowe stosują funkcje logowania za pomocą odcisku palca, czy identyfikacji twarzy, co uniemożliwia cyberprzestępcom pozyskanie hasła do konta.

8. PAMIĘTAJ O AKTUALIZOWANIU SYSTEMU, ORAZ OPROGRAMOWANIA NA SWOIM URZĄDZENIU MOBILNYM



ZAWSZE pamiętaj o aktualizacji systemu i oprogramowania antywirusowego. Systemy pełne są „dziur", przez które cyberprzestępcy mogą się dostać do Twojego konta, dlatego tak ważne są uaktualnienia, które te „dziury" naprawiają. Z kolei oprogramowanie antywirusowe na wczesnym etapie pozwala wykryć złośliwe oprogramowanie i zabezpieczyć Twoje urządzenie mobilne przed atakiem cyberprzestępcy.

9. MONITORUJ AKTYWNOSĆ NA RACHUNKU BANKOWYM

Sprawdzaj datę ostatniego logowania do bankowości elektronicznej. Pozwoli to wykryć czy ktoś obcy nie logował się do Twojego elektronicznego konta bankowego. Wczesne rozpoznanie może uratować zgromadzone środki. Jeśli taka sytuacja się wydarzy, natychmiast zmień hasło do konta i zgłoś sprawę do banku.

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