
**Haki na cyberataki**

# Bezpieczne Fin@nse

**cz. 1 Bezpieczne korzystanie z e-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. 1 Poradnika Bezpieczne Fin@nse Bezpieczne korzystanie z e-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. 1 Bezpieczne korzystanie z e-bankowości

### 1. NIGDY NIE OTWIERAJ STRON DO LOGOWANIA W BANKU KLIKAJĄC W LINK DO NICH KIERUJĄCY


Phishing to jedna z najpopularniejszych metod włamania na konto bankowe. Polega na podszywaniu się cyberprzestępcy pod bank w celu wyłudzenia od konkretnej osoby niezbędnych informacji, albo skłonienia jej do określonych działań. Cyberprzestępca tworzy identyczną stronę jak strona bankowa o bardzo podobnym adresie WWW. Następnie wysyła wiadomość e-mail z podstawionym (fałszywym) linkiem, albo zamieszcza reklamę w Internecie, lub wyszukiwarkach w celu wyłudzenia (złowienia) nieświadomych ofiar.
Nieświadomy użytkownik podaje login, oraz hasło a czasem nawet otrzymany kod SMS, który umożliwia dokonanie transakcji ze swojego konta na rzecz cyberprzestępcy. Dlatego, wchodząc na stronę bankową ZAWSZE wpisuj ją ręcznie i sprawdzaj czy jest zabezpieczona i zaszyfrowana (certyfikat zgodności – zamknięta kłódka).

2. **NIE KORZYSTAJ Z BANKOWOŚCI ELEKTRONICZNEJ W SIECIACH OGÓLNIE DOSTĘPNYCH (DARMOWYCH)**


Sieci ogólnodostępne (darmowe) są ulubionym miejscem ataków cyberprzestępców. Są tam wyjątkowo anonimowi, ponieważ trudniej ustalić z jakiego konkretnego urządzenia lub lokalizacji nastąpił ich atak. Nigdy nie ma pewności, czy sieci nie są podsłuchiwane przez cyberprzestępców, którzy mogą przechwycić informacje wysyłane przez Ciebie do serwisów zewnętrznych np. login i hasło do logowania do bankowości elektronicznej.

3. **NIGDY NIE KORZYSTAJ Z BANKOWOŚCI ELEKTRONICZNEJ NA URZĄDZENIACH, KTÓRE NIE SĄ ZAUFANE**

Nigdy nie ufaj urządzeniu nad którym nie masz kontroli, które nie jest Twoje. Nigdy nie wiadomo, czy komputer znajomego z pracy, lub znajomej z sąsiedztwa nie ma zainstalowanych wirusów i innych programów szpiegujących. Jeżeli nie ma takiej potrzeby, NIGDY nie korzystaj z bankowości elektronicznej na nie swoim urządzeniu (komputer, laptop, tablet).

4. **JEŻELI KORZYSTASZ Z BANKOWOSĆI ELEKTRONICZNEJ, UPEWNIJ SIĘ, ŻE POSIADASZ AKTUALNĄ, ORAZ AKTYWNĄ OCHRONĘ PRZECIWWIRUSOWĄ**


Wirusy, oraz programy szpiegujące to bardzo popularna przyczyna nieświadomego przekazania danych do logowania na konto cyberprzestępcy. Mogą one także modyfikować adres serwerów pod którym znajduje się m.in. strona banku celem przekierowania ruchu na stronę podstawioną. ZAWSZE miej zabezpieczenie w postaci programu antywirusowego. Uaktualniaj bazę wirusów, oraz skanuj regularnie urządzenia.

5. **REGULARNIE ZMIENIAJ HASŁO DO BANKOWOŚCI ELEKTRONICZNEJ MINIMUM RAZ NA MIESIĄC**


Regularna zmiana hasła dostępu to jedna z lepszych metod zapobiegania włamaniom na Twoje konto bankowe.

## 6. ZAWSZE UŻYWAJ UNIKALNEGO I SILNEGO HASŁA


Cyberprzestępca posiadają dostęp do milionów standardowych haseł. Używając prostych haseł, ułatwiasz im zadanie. W haśle NIGDY nie używaj imion czy nazwisk swoich najbliższych. NIGDY nie używaj numerów identyfikacyjnych takich jak np. numer PESEL lub dat urodzenia. Hasło powinno być długie, zawierać znaki specjalne takie jak @, #, $, !, %, spacje, cyfry, oraz przynajmniej jedną literą pisaną dużą A, B, C, itd. i powinno mięć formę zdania (dłuższa forma). W przypadku liter nie stosuj ciągu występujących po sobie znaków np. qwerty (na klawiaturze). Ta sama zasada obowiązuje w przypadku cyfr np. 78963 (klawiatura numeryczna).

## 7. NIGDY NIE PUBLIKUJ SWOJEGO NUMERU TELEFONU SLUŻĄCEGO DO UWIERZYTELNIANIA I ZATWIERDZANIA TRANSAKCJI

Cyberprzestępca dysponujący dostępem do Twojego rachunku, potrzebuje kodu z wiadomości SMS do potwierdzenia transakcji. Jeśli pozna Twój numer telefonu, również może podmienić wiadomości weryfikacyjne z banku.

## 8. ZAWSZE WERYFIKUJ KODY Z WIADOMOŚCI SMS


Cyberprzestępca dysponujący dostępem do Twojego rachunku potrzebuje kodu z wiadomości SMS do potwierdzenia transakcji. Jeśli pozna Twój numer telefonu, może podmienić wiadomości weryfikacyjne z banku. ZAWSZE pamiętaj, żeby dokładnie czytać tego typu wiadomości SMS i sprawdzać, czy zgadza się kwota operacji oraz numer rachunku odbiorcy.

## 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.

## 10. W PRZYPADKU ZGUBY TOKENA LUB TELEFONU, NA KTÓRY WYSYŁANE SĄ SMSY UWIERZYTELNIAJACE TRANSAKCJĘ, NATYCHMIAST ZABLOKUJ TEN ŚRODEK AUTORYZACJI

Zguba jednego z tych przedmiotów powinna skutkować zablokowaniem sposobu uwierzytelniania transakcji w banku. Blokady można dokonać on-line, telefonicznie i w oddziale u doradcy.

## 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