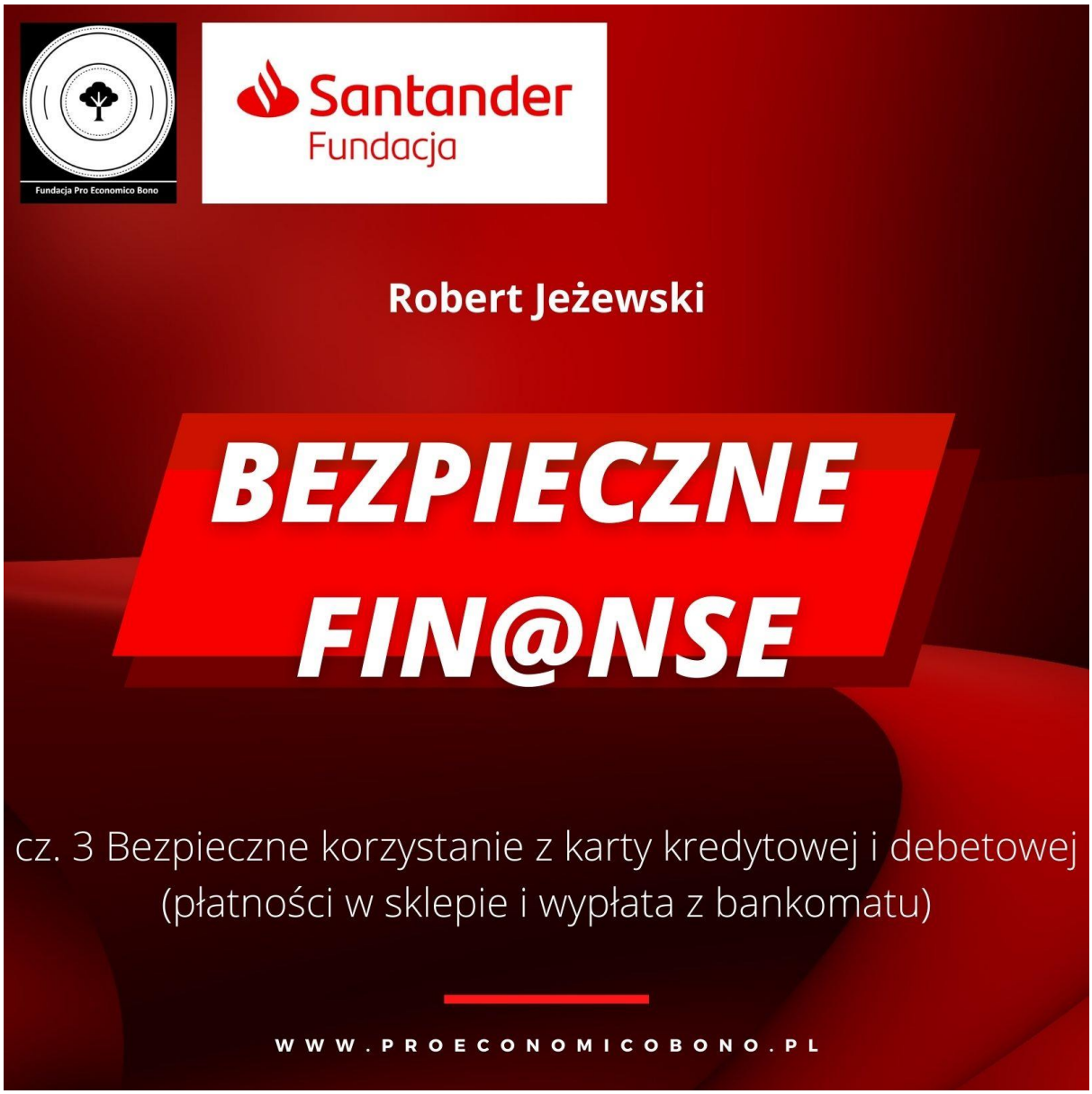


Haki na cyberataki

Bezpieczne Fin@nse

cz. 3 Bezpieczne korzystanie z karty kredytowej i debetowej (płatności w sklepie i wypłata z bankomatu)

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. 3 Poradnika Bezpieczne Fin@nse Bezpieczne korzystanie z karty kredytowej i debetowej (płatności w sklepie i wypłata z bankomatu)

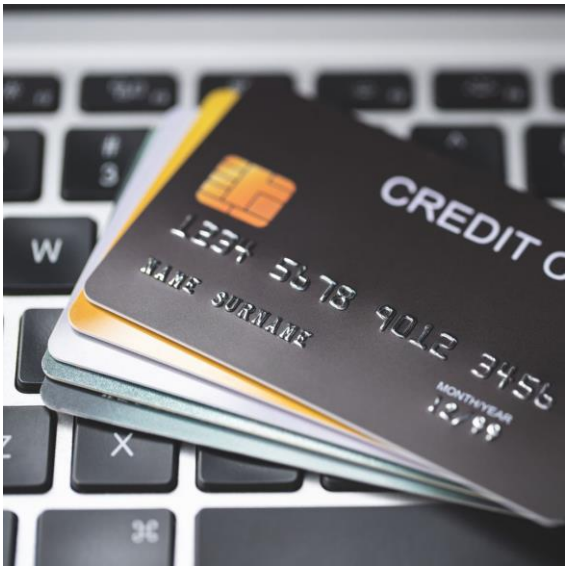
Zapraszam do lektury i zgłębiania tematu, jakże ważnego w dzisiejszym, bardzo dynamicznym otoczeniu.

prof. ucz. dr inż. Robert Jeżewski

Prezes Zarządu Fundacji Pro Economico Bono

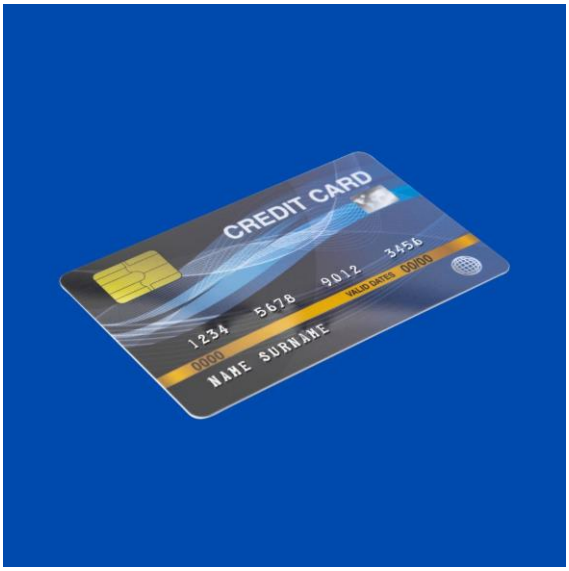
cz. 3 Bezpieczne korzystanie z karty kredytowej i debetowej (płatności w sklepie i wypłata z bankomatu)

1. ZAWSZE PILNUJ SWOJEJ KARTY PŁATNICZEJ



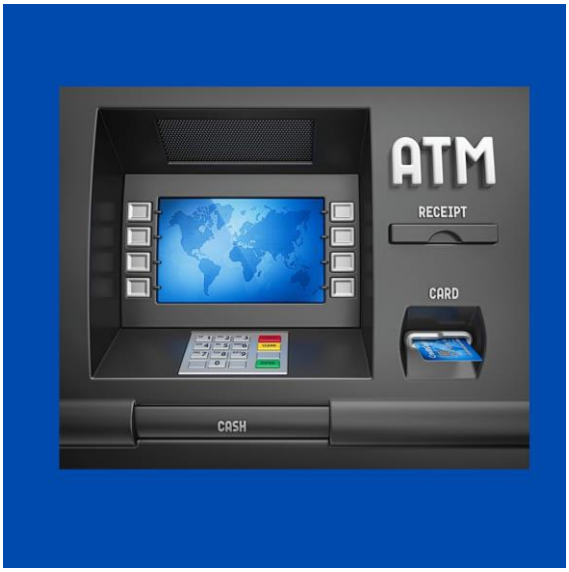
Za pomocą karty płatniczej wypłacasz pieniądze ze swojego banku. Zawsze jej pilnuj. W przypadku, kiedy nie możesz jej znaleźć, nie wpadaj w panikę. Zacznij poszukiwania od odzieży ostatnio używanej. W przypadku, kiedy poszukiwania okażą się bezskuteczne, od razu dzwoń do swojego banku i ją zastrzeż, oraz poproś o wyrobienie nowej.

2. NIGDY NIE SPUSZCZAJ KARTY Z OCZU



Na karcie są umieszczone newralgiczne dane, oraz nr CVV służący do płatności w Internecie. Nigdy nie dawaj nikomu postronnemu (kelnerowi w restauracji, kasjerowi w sklepie, itp.) swojej karty, tak że tracisz ją z zasięgu wzroku. Wtedy może nastąpić kradzież danych i ich wykorzystanie. Wtedy najlepiej udać się z taką osobą w miejsce, gdzie nastąpi płatność.

3. ZAWSZE UWAŻNIE OGLĄDAJ BANOMAT



Skimming to oszustwo polegające na zamontowaniu specjalnej nakładki na bankomacie. Na pierwszy rzut oka jest ona niewidoczna. Nakładka doczepiana jest do otworu, w który wsuwamy kartę płatniczą i zawiera skaner paska magnetycznego. Wkładając kartę do czytnika skaner kopiuje dane karty, która następnie jest nanoszona na drugą czystą kartę. Drugi element nakładki to fałszywa klawiatura do wpisywania kodu PIN. Po sczytaniu tych danych (dane karty i nr PIN), złodziej może wypłacać środki z bankomatu. Jeśli widzisz podejrzaną sytuację NIGDY nie wypłacaj środków o podejrzany bankomat zgłoś do banku.

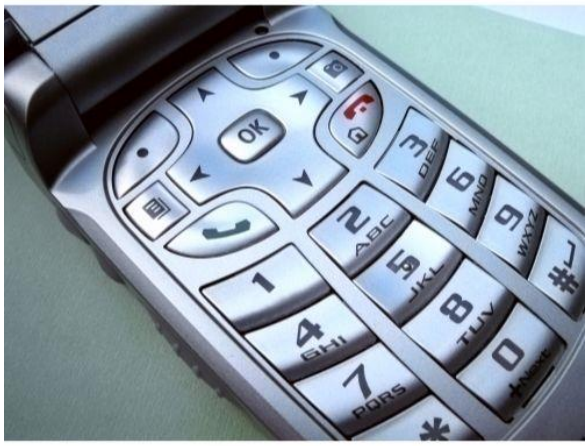
4. ZAWSZE USTAWIAJ LIMITY PŁATNOŚCI DLA SWOICH KART

Banki pozwalają swobodnie definiować limity transakcji na kartach płatniczych. Dla swojego bezpieczeństwa lepiej wprowadź limity dzienne. W przypadku kradzieży, złodziej nie wypłaci wszystkich środków a Ty będziesz miał okazję odpowiednio wcześniej zareagować.

5. USTAW POWIADOMIENIA NA RACHUNKU W POSTACI SMS

Powiadomienia SMS o transakcjach na rachunku bankowym są dobrym zabezpieczeniem przed złodziejami. Każda transakcja na rachunku jest monitorowana w postaci wysłanego SMS-a. W przypadku użycia karty przez osoby trzecie, od razu dowiesz się o nieuprawnionych ruchach na swoim rachunku i zdążysz odpowiednio wcześniej zareagować.

6. ZAPAMIĘTAJ LUB ZAPISZ NUMER DO CENTRUM ZASTRZEGANIA KART

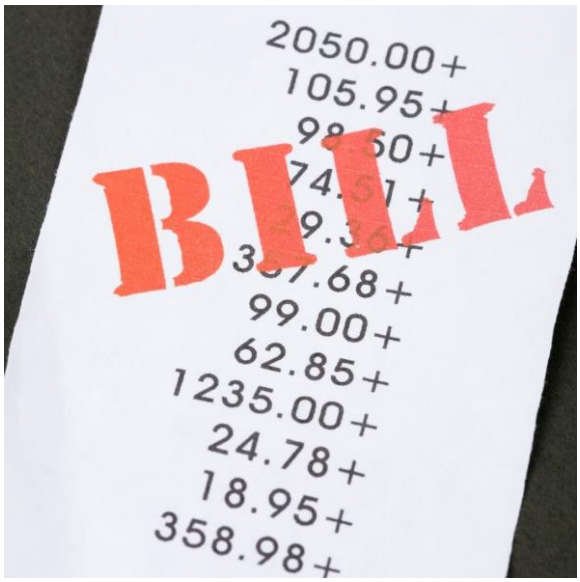


Numer do zastrzegania kart jest nadrukowany na rewersie każdej karty płatniczej. Dlatego warto odpowiednio wcześniej go sobie zapamiętać lub zapisać w telefonie. Funkcjonuje też uniwersalny numer, pod którym można zastrzec kartę dowolnej instytucji: **828 828 828**

7. ZAWSZE PAMIĘTAJ O ZABRANIU KARTY Z BANKOMATU

Za granicą można spotkać bankomaty, które najpierw wydają gotówkę, a następnie kartę (system funkcjonujący odwrotnie niż w Polsce). Jest to bardzo mylące w przypadku, kiedy osoba jest rozkojarzona lub się śpieszy. ZAWSZE pamiętaj o sprawdzeniu czy z bankomatu poza środkami zabrałeś też swoją kartę płatniczą.

8. ZAWSZE SPRAWDZAJ KWOTY NA RACHUNKU PRZY KASIE



W przypadku płatności kartą jesteśmy skłonni do rozrzutności i nie pilnujemy (nie pamiętamy) kwot, które wydajemy. Dlatego ZAWSZE sprawdzaj kwoty z rachunku z kwotami, które opłacasz kartą płatniczą. Na to liczą złodzieje, którzy wpisują inną kwotę na terminal niezgodną z kwotą na rachunku.

9. PODCZAS WPROWADZANIA NUMERU PIN ZAWSZE ZASŁANIAJ KALAWIATURĘ

Podczas płatności kartą lub wypłaty z bankomatu, zawsze zasłaniaj klawiaturę nie ujawniając swojego numeru PIN. W przypadku zgubienia karty lub jej zapomnienia przy płatnościach, złodziej będzie miał ułatwione zadanie. Nigdy nie wiesz, czy osoba stojąca za Tobą w kolejce jest uczciwa.

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