# OD NIEBEZPIECZNEGO ZAŁĄCZNIKA DO UTRATY NASZYCH PIENIĘDZY

## 1.

Atakujący wysyła do nas spam, czyli dużą liczbę wiadomości przy pomocy poczty elektronicznej lub portali społecznościowych, w celu skłonienia nas do odwiedzenia konkretnej strony internetowej lub podania osobistych danych (np. loginu i hasła do serwisu aukcyjnego czy konta bankowego).

## 2.

Spamer podszywa się pod znaną instytucję (np. bank) i uzasadnia konieczność zweryfikowania danych do konta internetowego procedurami bankowymi lub zablokowaniem konta. Link do strony internetowej spamera bardzo przypomina adres http konkretnego banku.

## 3.

W zależności od treści e-maila, nieświadomie podajemy swoje poufne dane lub wchodzimy na spreparowaną przez cyberprzestępcę stronę, która do złudzenia przypomina znaną nam witrynę.

## 4.

Na spreparowanej stronie logujemy się, myśląc, że mamy do czynienia z autentyczną witryną swojego banku albo serwisu aukcyjnego i nasze dane poufne zostają przechwycone przez cyberprzestępcę.


## 5.

Nasz komputer bądź smatrfon zostaje zarażony tzw. złośliwym oprogramowaniem (takim jak wirusy czy konie trojańskie) i dołącza do sieci komputerów, które są pod kontrolą podziemia internetowego.Od tej pory cybeprzestępca może kontrolować wszystko, co robi na komputerze jego właściciel oraz jest w stanie dokonywać nieuprawnionych transakcji w sposób niezauważalny dla użytkownika.


Rzecznik Finansowy
www.rf.gov.pl

CEO
CENTRUM EDUKACJI OBYWATELSKIEJ