Jeden SMS może zrujnować

SMS wyglądający na pierwszy rzut oka jak informacja z banku może narazić nas na utratę wszystkich oszczędności. Tak samo niebezpieczne mogą być maile na przykład z informacją o zablokowaniu dostępu do konta i konieczności pilnej weryfikacji danych. Złodzieje potrafią doskonale podszyć się pod różne instytucje i wiedzą jak napisać wiadomość żeby skłonić nas do kliknięcia w link prowadzący do fałszywej strony.

Kiedyś złodzieje kojarzyli się głownie z osiłkami, którzy czaili się na ofiarę gdzieś w ciemnym zaułku z łomem w ręku. Dziś jednak tego typu rabusie stanowią rzadkość. Ich miejsce zajęli cyberprzestępcy, ludzie o wiele inteligentniejsi i kulturalniejsi od swoich kolegów zajmujących się „analogowymi kradzieżami".

Najgroźniejsze dla nas grupy przestępcze tworzą znakomici znawcy psychologii i bardzo dobrze wykształceni inżynierowie. Ich sztuczki są tak dopracowane, że praktycznie każdy może się na nie nabrać. Najlepszym przykładem jest to jak hakerzy zaatakowali np. komitet wyborczy kandydującej na urząd prezydenta Stanów Zjednoczonych Hilary Clinton. Członkowie sztabu otrzymali wiadomość, że ich hasła e-mail straciły ważność i w związku z tym proszeni są o wygenerowanie nowych. Oczywiście w sprytnie przygotowanym mailu podano link do odpowiednio spreparowanej przez hakerów witryny. Na tę sztuczkę dał się nabrać m.in. szef sztabu Clinton, który w ten sposób podał cyberprzestępcom swoje hasło do konta mailowego. W efekcie jego naiwności wykradziono wszystkie informacje dotyczące kampanii prezydenckiej kandydatki.

Większość ataków polega właśnie na wykorzystaniu ludzkiej naiwności. Tworzy się komunikat zmuszający odbiorcę do tego żeby wykonał szybko jakieś działanie. Nikt nie chce stracić dostępu do maili albo mieć zablokowanego konta bankowego. Dlatego klikamy w podany link żeby uchronić się przed takim „nieszczęściem". I robimy to choć powinniśmy pamiętać, że banki nigdy nie komunikują się z nami w ten sposób.

Czy można uchronić się przed takimi kłopotami? Najlepsza rada, to po prostu nie klikać od razu w link, chwilę pomyśleć, zadzwonić do instytucji od której potencjalnie otrzymaliśmy e-mail lub smsa, z pytaniem czy rzeczywiście chcą żebyśmy wykonali jakieś działania.

Warto również zabezpieczyć się przed możliwością przejęcia naszych urządzeń elektronicznych przez hakerów. To znaczy, że jeśli wykorzystujemy smartfon do wykonywania operacji bankowych, nie powinno się instalować na nim żadnych innych aplikacji, zwłaszcza związanych z mediami społecznościowymi, gier itp. Mogą one bowiem spowodować wyciek danych lub doprowadzić do przejęcia urządzenia przez cyberprzestępcę.

Warto również rozdzielić kanały komunikacyjne, tak by autoryzujące wiadomości SMS przychodziły na inne urządzenie, niż to przez które logujemy się do banku. Dzięki temu jeżeli nawet *malware*, czyli złośliwe oprogramowane, zostanie przez nas zainstalowane to i tak atakujący nie uzyska dostępu do naszego konta bankowego, ponieważ albo nie będzie mógł przeczytać haseł albo nie zaloguje się do aplikacji bankowości elektronicznej.

Warszawski Instytut Bankowości