

Warto przypominać je użytkownikom bankowości internetowej :

1. Używaj filtru antyspamowego

- większość oszustw rozpoczyna się od niezamówionej wiadomości reklamowej. Filtr spamu, który znajduje się w praktycznie każdym współczesnym programie pocztowym oraz w większości usług *webmail* powinien zatrzymać prawie wszystkie takie wiadomości.

2. Nieoczekiwane i niezamówione wiadomości e-mail traktuj z ostrożnością

- nie wierz w każdą wiadomość, jaką otrzymasz z internetu. Nie otwieraj załączników, których nie oczekujesz. Nawet wiadomość ze znanego ci adresu może zawierać złośliwe oprogramowanie. Nigdy nie klikaj na odnośniki umieszczone w wiadomościach od nieznanych ci nadawców.

3. Uważaj na załączniki do wiadomości e-mail

- załączniki do wiadomości e-mail to jeden z najłatwiejszych sposobów na rozpowszechnianie wirusów komputerowych. Mogą one ułatwić wykradzenie informacji z twojego komputera lub, co gorsza, zmienić twój komputer w część służącej do ataków internetowych sieci *botnet*. Nawet znany ci adres nie gwarantuje bezpieczeństwa załącznika - twój znajomy również mógł paść ofiarą wirusa.

4. Zachowuj zdrowy rozsądek

- jeśli ktoś nieznanymi oferuje ci w wiadomości e-mail przekazanie fortuny, żąda opłaty za złamanie jakiegoś przepisu lub prosi o pomoc w przekazaniu pieniędzy z odległego kraju, zastanów się, czy na pewno takie wiadomości są wiarygodne.

5. Zainstaluj i często aktualizuj program antywirusowy

- jeśli jeszcze nie masz programu antywirusowego, zainstaluj go jak najszybciej. Upewnij się, że ma funkcję automatycznej aktualizacji i włącz ją. Jeśli twój program antywirusowy oferuje skanowanie wiadomości e-mail, włącz tę funkcję.

6. Zainstaluj i aktualizuj osobistą zaporę sieciową

- zaporę sieciową (firewall) w żaden sposób nie chroni przed zagrożeniami płynącymi z niebezpiecznych wiadomości e-mail. Mimo to należy ją zainstalować. Jeśli przypadkiem otworzysz załącznik z wirusem, zaporę sieciową nie pozwoli mu kontaktować się z

przestępcami. Twój komputer nie weźmie też udziału w atakach używających zainfekowanych maszyn. Podejrzone próby kontaktu z internetem sygnalizowane przez zaporę sieciową mogą wskazać ci złośliwy program w twoim komputerze.

7. Poznaj zasady komunikacji przez e-mail instytucji, z którymi współpracujesz

- większość instytucji ma jasne zasady dotyczące komunikacji przez e-mail (na przykład, twój bank na pewno nie poprosi cię o wysłanie jakichkolwiek informacji tą drogą). Znajomość tych zasad pomoże ci wykryć fałszywe wiadomości. Przy okazji: pamiętaj, że wysyłanie tajnych danych przez nieszyfrowany e-mail zawsze jest niebezpieczne.

8. Skonfiguruj swój program do odbioru poczty e-mail pod kątem bezpieczeństwa

- twój program pocztowy oraz usługa *webmail* mogą być nieco bezpieczniejsze. Warto na przykład zmienić format otrzymywanych wiadomości z HTML na tekstowy. Dzięki temu unikniesz niebezpiecznego kodu ukryte.

(źródło : Miesięcznik finansowy BANK nr 12)2009)