



Jak nie dać się złowić w sieci, czyli o bezpiecznym bankowaniu

Cel: kształtowanie postawy bezpiecznego korzystania z sieci, zapoznanie dzieci z bankowością internetową.

Rozwój nowych technologii w trwały sposób zmienił nasze życie, także w sferze finansów. Zarządzanie domowym budżetem, opłacanie rachunków bez potrzeby wychodzenia z domu, płatności kartą, telefonem, czy BLIK-iem są dziś powszechne. By bankowanie w sieci było bezpieczne, należy stosować się do zasad, które, choć powinny być powszechnie znane, nadal wymagają przypomnienia. Poniżej ściągawka dla rodzica. Warto do niej zajrzeć przed rozmową z dzieckiem, a przy okazji sprawdzić, na ile my sami stosujemy te wszystkie zasady w codziennym życiu.

ZASADA	SAMOOCENA		
	ROBIĘ TAK ZAWSZE LUB PRAWIE ZAWSZE	ROBIĘ TAK CZĘSTO	ROBIĘ TAK RZADKO LUB PRAWIE NIGDY TAK NIE ROBIĘ
1. Nie podaję nikomu danych do logowania do serwisu internetowego ani aplikacji, nie zapisuję nigdzie haseł, nie udostępniam ich drogą internetową.			
2. Zmieniam regularnie hasło do logowania; tworzę hasła trudne do odgadnięcia (zawierające cyfry, małe i duże litery, znaki specjalne) oraz takie, których nie używam w innych serwisach.			
3. Nie udostępniam innym osobom swojego urządzenia elektronicznego, którego używam do autoryzacji operacji w banku.			

ZASADA	SAMOCENA		
	ROBIĘ TAK ZAWSZE LUB PRAWIE ZAWSZE	ROBIĘ TAK CZĘSTO	ROBIĘ TAK RZADKO LUB PRAWIE NIGDY TAK NIE ROBIĘ
4. Sprawdzam przed zalogowaniem czy adres strony zaczyna się od https://... oraz czy pojawia się symbol kłódki.			
5. Nie instaluję ani nie uruchamiam programów przesyłanych e-mail'em; nie otwieram plików, których pochodzenia nie znam (np. przesłanych przez nieznaną mi osobę).			
6. Nie podaję poufnych danych drogą elektroniczną (np. w odpowiedzi na maila lub telefon).			
7. W razie zagubienia karty lub innych zagrożeń mojej bankowości internetowej, natychmiast blokuję do niej dostęp.			
8. Chronię swoje urządzenia przed wirusami. Używam tylko sprawdzonych i legalnych programów antywirusowych.			
9. Korzystam z Internetu tylko na zaufanych urządzeniach i w ramach bezpiecznych sieci.			
10. W razie podejrzanych telefonów (np. z prośbą o pilny przelew gotówki), weryfikuję informację np. w banku lub na policji.			

Jeśli przy jakiejś zasadzie nie dało się zaznaczyć „Robię tak zawsze lub prawie zawsze”, to takie postępowanie wymaga natychmiastowej korekty. Zwiększa ono bowiem ryzyko kradzieży i wykorzystania naszych danych osobowych oraz pieniędzy.

Warto również pamiętać, że same banki dodatkowo dbają o bezpieczeństwo użytkowników swoich serwisów online. Bankowe systemy internetowe i aplikacje mobilne chronione są szeregiem nowoczesnych i ciągle udoskonalanych zabezpieczeń, które zapewniają optymalne bezpieczeństwo i zarazem wygodę podczas codziennego bankowania. Banki stosują m.in: unikatowe dane do logowania, maskowane hasła, przypomnienia o cyklicznej zmianie hasła do logowania. Transakcje w serwisie bankowym zabezpieczone są dodatkową autoryzacją, istnieje możliwość ustanawiania ich limitów. Dostępne są również usługi wspierające monitorowanie

zdarzeń na koncie i stanu finansów. Przykładowo w Banku Millennium, po zalogowaniu do aplikacji mobilnej czy serwisu internetowego, użytkownik widzi sekcję „Wydarzenia” pokazującą ostatnie zdarzenia na koncie. Wystarczy jeden rzut oka, by sprawdzić saldo – również na kontach w innych bankach! Jednym ruchem myszki można zablokować kartę płatniczą (gdy np. zawieruszy się w portfelu) i równie łatwo odblokować ją bez potrzeby zamawiania nowej. Dodatkowo możliwe jest ustawienia powiadomień w telefonie, które zasygnalizują przelew z konta czy płatność kartą. To jedynie niektóre z wybranych sposobów na bezpieczne bankowanie online. Warto z nich korzystać!

Oczywiście nasze maluchy nie będą w stanie zapamiętać tak wielu informacji. Najczęściej nie są im też potrzebne w codziennym funkcjonowaniu. Nie oznacza to jednak, że nie powinniśmy rozmawiać o nich z dziećmi. Przedszkolaki bardzo aktywnie korzystają z internetu, dlatego kształtowanie pewnych nawyków – istotnych dla bezpiecznego bankowania – warto rozpocząć już u 3–4-latka.

Spśród wymienionych zasad dla dzieci w wieku przedszkolnym najbardziej istotne i łatwe do zrozumienia będą cztery:

- zabezpiecz hasłem dostęp do komputera, tabletu bądź telefonu (udostępnij je jedynie rodzicom),
- nie podawaj nikomu swoich danych osobowych (nazwiska, adresu zamieszkania, nazwy przedszkola) ani nie udostępniaj w sieci swoich zdjęć,
- korzystaj z jedynie z zaufanej sieci (unikaj łączenia się z publiczną siecią np. w kawiarni czy pociągu) wg reguł ustalonych z rodzicami (np. ilość czasu, sposób korzystania),
- często sprawdzaj z rodzicem, czy komputer, tablet, telefon nie ma wirusów lub innych niebezpiecznych plików; rozmawiaj z rodzicem o tym, co danego dnia robiłeś w internecie.

Zasady te można przygotować w formie umowy – kontraktu, który podpisuje i dziecko, i rodzice.

Kolejnym krokiem powinna być konsekwentna realizacja zasad – tak, by dla dziecka stały się „normalnym” (powszechnym i niemal odruchowym) sposobem korzystania z internetu. Kiedy tak się stanie, rodzic może zacząć wprowadzać dziecko w świat bankowości elektronicznej, tj. pokazać mu, jak w praktyce wygląda bankowość elektroniczna i razem z nim np. dokonać przelewu (lub nawet kilku), zwracając uwagę za zasady bezpieczeństwa.



Starszym dzieciom można pozwolić na posiadanie własnych produktów bankowych i własnej bankowości elektronicznej. Powinny one jednak najpierw uczyć się korzystania z niej pod ścisłym nadzorem rodzica, a dopiero potem samodzielnie. W jakim wieku? Prawo stanowi, że od 13. roku życia. Wtedy dziecko dobrze już sobie radzi z obliczeniami matematycznymi, rozwija myślenie symboliczne (jest w stanie wyobrazić sobie wirtualne pieniądze i transakcje), a także rozumie moralne pojęcie „dobra” i „zła” (niebezpieczeństwo ze strony innych, nieznanych, korzystających z internetu osób; konsekwencje udostępnienia komuś hasła do konta itp).

Do poduszki polecamy zaś bajki:

„Powiedz komuś!” autorstwa E. Zubrzyckiej,
 „Znajomy taty”, „Pierwsze spotkanie” (bajki dostępne na www.superkid.pl/zasady-bezpieczenstwa-dla-dzieci),
 „Nieprawdziwy świat” i „Wirtualny nieprzyjaciel” autorstwa K. Wojas.