Broszura stanowi materiał dodatkowy do gry "Haki na cyberataki" przygotowanej przez Stowarzyszenie Ochrony Konsumentów Aquila i sfinansowanej dzięki darowiźnie udzielonej w ramach programu grantowego "Haki na cyberataki", organizowanego przez Fundację Santander Bank Polska

HAKI NA CYBERATAKI

Część I

- ⇒ **Bezpieczni w sieci**
- ⇒ **Mikropłatności**
- ⇒ **Kryptowaluty**
- ⇒ **Subskrypcje**

Santander Fundacja

Broszura stanowi materiał dodatkowy do gry "Haki na cyberataki" przygotowanej przez Stowarzyszenie Ochrony Konsumentów Aquila i sfinansowanej dzięki darowiźnie udzielonej w ramach programu grantowego "Haki na cyberataki", organizowanego przez Fundację Santander Bank Polska

Bezpieczni w sieci

1. Hasła pozwalają nam zabezpieczać dane, które nie powinny trafić w niepowołane ręce. Hasłem powinien być zabezpieczony nasz komputer/laptop/notebook, jak również smartfon.
2. Nie zapisuj hasła w widocznym miejscu. Zapisywanie haseł na karteczce i trzymanie go np. w etui telefonu, w portfelu, przypięte w formie karteczki do komputera w pracy, na obudowie laptopa to zaproszenie do włamania się na Twój komputer.
3. Stosuj silne hasła, unikaj zbyt prostych np. 1234, QWERTY. Silne hasło to takie, które ma minimum 8 znaków (im więcej tym lepiej), powinno zawierać duże i małe litery, cyfry, spacje oraz znaki specjalne. Dobrym pomysłem są tzw. hasła frazowe, tzn. składające się z kilku całkowicie przypadkowo dobranych słów.
4. Nie używaj tych samych haseł do różnych kont. Im bardziej różnią się Twoje hasła, tym mniejsza szansa na ich złamanie „przy okazji”.
5. Unikaj wpisywania haseł podczas korzystania z publicznie dostępnych sieci (np. wi-fi w galerii handlowej, restauracji).
6. Unikaj wpisywania haseł w miejscach publicznych (autobus, restauracja, centrum handlowe, dworzec). Osoba stojąca za Tobą lub mająca dostęp do kamery może zobaczyć jakie dane wpisujesz.
7. Zabezpiecz odpowiednio swój smartphone. Możesz używać kodu PIN, symbolu do narysowania na ekranie, rozpoznawania linii papilarnych. Pamiętaj jednak, że te sposoby nie zawsze są bezpieczne. Skan twarzy to gadżet, a nie realne zabezpieczenie. Lepszym zabezpieczeniem jest rozpoznawanie tęczówki, jednak w nowszych modelach odchodzi się od tej technologii.

Santander Fundacja

8. Jakie mogą być konsekwencje kradzieży niewystarczająco zabezpieczonego smartfona, na którym mamy zapisane hasła do portali społecznościowych, maili, a w szczególności kont bankowych? Kradzież smartfona może się okazać początkiem większych problemów. Wyczyszczenie konta bankowego, kradzież tożsamości, dostęp do naszych zdjęć – to wszystko może nas spotkać, jeśli nie zabezpieczymy odpowiednio naszego telefonu. Przestępca, który zdobędzie nasze dane, może bez problemu wziąć kredyt/pożyczkę na nasze nazwisko. My zostaniemy z długiem i problemami. Nasze dane (wraz ze smartfonem) mogą również posłużyć do popełniania przestępstw w sieci. Tłumaczenie organom ścigania, że to nie my, to długotrwały i nieprzyjemny proces.

9. Phishing to cyberatak, w trakcie którego przestępcy podszywając się pod np. banki, urzędy, firmy kurierskie, operatorów telekomunikacyjnych, a nawet naszych znajomych, starają się wyłudzić nasze dane do logowania np. do kont bankowych lub kont społecznościowych. Otrzymywane wiadomości są starannie przygotowywane (często przestępcy używają podobnych do autentycznych nazw witryn) i wyglądają na autentyczne, choć naprawdę są fałszywe. Przestępcy próbują skłonić nas do ujawnienia poufnych informacji, przesyłają link do strony internetowej rozprzestrzeniającej szkodliwe oprogramowanie lub zainfekowany załącznik. Nie klikaj w przesyłane linki - banki i inne instytucje w swoich wiadomościach nigdy nie zamieszczają linków do strony logowania lub do bramek płatniczych.

10. Chargeback (z ang. obciążenie zwrotne) to procedura odzyskiwania pieniędzy w przypadku błędnie realizowanych lub budzących wątpliwości transakcji. Można z niej skorzystać tylko wtedy, gdy **płaciliśmy kartą płatniczą**. Chargeback przeprowadza **bank**. Aby rozpocząć tę procedurę, musimy złożyć reklamację do naszego banku

Broszura stanowi materiał dodatkowy do gry "Haki na cyberataki" przygotowanej przez Stowarzyszenie Ochrony Konsumentów Aquila i sfinansowanej dzięki darowiźnie udzielonej w ramach programu grantowego "Haki na cyberataki", organizowanego przez Fundację Santander Bank Polska

i wskazać w niej uzasadnione powody do zwrotu pieniędzy (np. kupiony produkt nie został dostarczony, padliśmy ofiarą oszustwa).

Mikropłatności

Mikropłatności to dokonywane w szybki sposób na niewielkie (czasem kilkugroszowe) kwoty płatności w sieci. Możemy w ten sposób nabywać np. dostęp do muzyki, filmów. Bardzo popularne są mikropłatności w grach sieciowych. Są dokonywane często **impulsywnie w dużych ilościach**, co powoduje bardzo duże **straty finansowe** po stronie graczy i bardzo duże zyski producentów gier. Zdarza się, że bez dokonania szeregu mikropłatności nie da się przejść gry – jest tu wykorzystany cały szereg trików mających zachęcić czy wręcz uzależnić gracza od ciągłego dokonywania mikropłatności.

Kryptowaluty

Kryptowaluta to waluta w pełni elektroniczna, nie emitowana przez żadne państwo. Istnieje **wyłącznie wirtualnie** i można z niej korzystać wyłącznie w płatnościach elektronicznych. Z uwagi na brak gwarancji państwowych oraz wysokie ryzyko zmiany kursu, korzystanie z kryptowalut jest **ryzykowne**.

Subskrypcje

Subskrypcja to cykliczna zapłata za dostęp do usługi. Należy zawsze mieć świadomość, że płatność za subskrypcję przebiega **bez naszego udziału** – pieniądza pobierane są z naszego konta **automatycznie**. Aby skutecznie zrezygnować z subskrypcji należy wypowiedzieć umowę. Samo usunięcie konta, czy wyłączenie subskrypcji może być **niewystarczające**.