OUCH! | Listopad 2015

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM WYDANIU..

- **Fałszywe sklepy online**
- **Bezpieczny komputer / urządzenie mobilne**
- **Karta kredytowa**

Bezpieczne zakupy w sieci

Sezon na ostrożność

Wielkimi krokami zbliża się czas przedświąteczny i już wkrótce mnóstwo osób zajmie się poszukiwaniem prezentów dla rodziny i przyjaciół. Wiele z nich, poszukując okazji i chcąc uniknąć tłumów, wybierze zakupy online. Niestety jest to także ulubiony czas przestępców na dokonywanie przetkrętów i oszustw. W tym numerze OUCH! opisujemy niektóre z zagrożeń związanych z zakupami online oraz przedstawiamy jakimi metodami chronić się przed oszustami.

Redaktor gościnny

Jonathan Homer (**@JonathanLHomer**) jest znanym liderem w zagadnieniach zwiększania świadomości wiedzy o cyberbezpieczeństwie zarówno w sektorze rządowym jak i prywatnym. Jon jest specjalistą od wiodących technik szkoleniowych i angażowania słuchaczy.

Fałszywe sklepy internetowe

Większość sklepów online jest oczywiście legalna lecz istnieją takie, które są fałszywymi stronami internetowymi przygotowanymi przez przestępców. Takie fałszywe strony powstają przez skopiowanie wyglądu i wykorzystaniu nazwy stron znanych sklepów. Gdy taka strona już funkcjonuje, oszuści starają się przyciągnąć do niej użytkowników szukających najbardziej korzystnej cenowo oferty. Podczas wyszukiwania najniższych cen w Internecie możesz zostać przekierowany na jedną z tych fałszywych stron internetowych.

Wybierając sklep internetowy albo serwis aukcyjny w celu kupna jakiejś rzeczy, zachowaj ostrożność w przypadku tych, które oferują wyjątkowo niskie ceny w porównaniu do innych, dobrze Ci znanych miejsc. Powodem, dla którego różnica w cenie może być tak duża może byc to, że po zakupie możemy otrzymać towar podrobiony, kradziony albo po prostu nie otrzymać go w ogóle. Ochroń się przed takimi sytuacjami postępując zgodnie z poniższymi zaleceniami:

- Sprawdź, czy na stronie jest podany istniejący adres i numer telefonu do działu sprzedaży lub wsparcia, do których można skierować pytania. Jeśli witryna wygląda podejrzanie, zadzwoń tam i porozmawiaj z osobą.
- Zwróć uwagę na oczywiste wskazówki, takie jak rażące błędy gramatyczne i ortograficzne.
- Zachowaj ostrozność jesli strona internetowa do złudzenia przypomina stronę innego dobrze znanego sklepu internetowego lub serwisu aukcyjnego, ale jej adres różni się od oryginalnego tylko w niewielkim stopniu (np. jedną literą). Na przykład, zazwyczaj odwiedzasz stronę https://amazon.com robiąc zakupy w sklepie Amazon. Ale czerwona lampka powinna zapalić się jesli znajdziesz się na stronie internetowej, udającej Amazon pod adresem http://store-amazon.com.
- Wpisz nazwę sklepu lub adres URL do wyszukiwarki i zobacz, co inne osoby napisały o tej stronie w przeszłości.

Bezpieczne zakupy w sieci

Zwróć uwagę na takie części opisów jak “oszustwo”, “nigdy więcej” lub “fałszywy”. Brak opinii to też nie jest dobry znak, ponieważ oznacza, że strona jest bardzo nowa.

Pamiętaj, że jeśli strona wygląda profesjonalnie, nie oznacza od razu, że jest prawdziwa. Jeśli jakiś aspekt serwisu wydaje Ci się podejrzany, lepiej poświęcić trochę czasu na sprawdzenie, czy sklep nie jest próbą oszustwa. Jeśli nie masz pewności czy sklep jest prawdziwy, to po prostu z niego nie korzystaj. Zamiast ryzykować, lepiej skorzystać ze sprawdzonego sklepu, co do którego masz pewność, nawet jeśli cena szukanego towaru nie jest aż tak atrakcyjna. Wówczas masz szansę otrzymać oryginalny produkt a Twój wyciąg z karty kredytowej będzie bez niespodzianek.

Ochroń się robiąc zakupy on-line tylko na zaufanych stronach o dobrej reputacji.

Bezpieczny komputer / urządzenie mobilne

Robienie zakupów tylko w bezpiecznych sklepach nie uchroni nas w zupełności przed próbami kradzieży danych lub pieniędzy. Również komputer, który jest wykorzystywany do robienia zakupów online musi być bezpieczny. Przestępcy próbują infekować komputery na różne sposoby, aby zdobyć numery kart kredytowych, dane logowania do serwisów bankowych i innych ważnych usług. Podejmij nastepujące kroki, aby Twoje urządzenia były bezpieczne:

- Jeśli masz w domu dzieci, rozważ korzystanie z różnych urządzeń dla dzieci i dla dorosłych. Dzieci są ciekawskie i interaktywnie korzystają z technologii, a w rezultacie są bardziej skłonne do zainfekowania urządzenia, z którego korzystają. Dzięki osobnemu urządzeniu tylko do transakcji internetowych, takich jak bankowość i zakupy, można zmniejszyć ryzyko zainfekowania. Jeżeli odrębne urządzenie nie jest rozwiązaniem w Twoim przypadku, stwórz oddzielne konta na wspólnym komputerze, i skonfiguruj je tak aby dzieci nie miały na nim uprawnień administracyjnych.
- Łącz się tylko z sieciami bezprzewodowymi którymi zarządzasz, takimi jak Twoja sieć domowa lub sieci o których wiesz, że możesz ufać dokonując transakcji finansowych. Korzystanie z publicznych sieci Wi-Fi, takich jak w lokalnej kawiarni może być świetne do czytania wiadomości, ale nie do dostępu do konta bankowego.
- Zawsze instaluj najnowsze aktualizacje systemu operacyjnego i miej uruchomiony program antywirusowy z aktualną bazą szczepionek. To sprawi, że zainfekowanie Twojego urządzenia dla przestępców będzie o wiele trudniejsze.

Karta kredytowa

Zachowaj ostrożność korzystając z karty kredytowej. Sprawdzaj comiesięczne wyciągi płatności, aby szybko wykryć podejrzane transakcje. Powinno się to robić przynajmniej raz w miesiącu. Niektóre banki dają możliwość włączenia

Bezpieczne zakupy w sieci

powiadomień SMS albo email dla każdej realizowanej płatności od pewnej kwoty. Zalecamy uruchomienie takiej usługi, aby natychmiast otrzymywać informacje o wszelkich zmianach salda karty. Innym rozwiązaniem jest posiadanie oddzielnej karty wyłącznie do transakcji internetowych, dzięki czemu, w przypadku wycieku danych karty, jej wymiana nie będzie wpływać na resztę Twoich operacji. Jeśli podejrzewasz, że dane karty kredytowej zostały podane na fałszywej stronie internetowej, jak najszybciej zadzwoń do banku i zablokuj kartę. Dlatego też karty kredytowe są lepsze do zakupów online niż karty debetowe. Karty debetowe pobierają pieniędze bezpośrednio z konta bankowego i jeśli zostało popełnione oszustwo, może być znacznie trudniej otrzymać zwrot pieniędzy.

Istnieją również rozwiązania pozwalające na płacenie bez narażania swojej karty kredytowej. Rozważ korzystanie z serwisów pośredniczących w płatnościach, takich jak PayPal albo PayU, które nie wymagają ujawnienia numeru karty sprzedawcy.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.
Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Linki

5 kroków dla własnego bezpieczeństwa:	https://www.securingthehuman.org/ouch/2014#october2014
Jak zabezpieczyć domową sieć:	https://www.securingthehuman.org/ouch/2014#january2014
Zabezpiecz swój nowy tablet:	https://www.securingthehuman.org/ouch/2013#december2013
Porada dnia SANS:	https://www.sans.org/tip_of_the_day.php

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski