©Wydawnictwo UR 2017
ISSN 2080-9069
ISSN 2450-9221 online

„Edukacja – Technika – Informatyka" nr 3/21/2017
www.eti.rzeszow.pl
DOI: 10.15584/eti.2017.3.37

MARIUSZ NYCZ[1], **ALICJA GERKA**[2], **MIROSŁAW HAJDER**[3]

Edukacja w zakresie metod i środków ochrony tożsamości w sieci

Education in the Field of Methods and Means of Network Identity Protection

[1] Doktor inżynier, Politechnika Rzeszowska im. Ignacego Łukasiewicza, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, Polska
[2] Inżynier, Politechnika Rzeszowska im. Ignacego Łukasiewicza, Polska
[3] Doktor inżynier, Wyższa Szkoła Informatyki i Zarządzania w Rzeszowie, Polska

Streszczenie

W opracowaniu przedstawiono problematykę ochrony tożsamości oraz metody i środki zapewnienia bezpieczeństwa użytkowników. Autorzy zwracają uwagę na fakt, iż odpowiednia edukacja w zakresie ochrony tożsamości jest kluczowa dla zapewnienia bezpieczeństwa użytkowników sieci.

Słowa kluczowe: ochrona tożsamości, kradzież tożsamości, cyberbezpieczeństwo

Abstract

The paper presents the issues of identity protection as well as methods and means of ensuring user safety. The authors point out that providing an adequate education in the area of identity protection is crucial to ensure the safety of network users.

Keywords: identity protection, identity theft, cybersecurity

Wstęp

Uwzględniając postępującą informatyzację społeczeństwa oraz rosnące z pokolenia na pokolenie zaufanie do technologii, zapewnienie bezpieczeństwa użytkowników sieci, a co się z tym wiąże, zapewnienie odpowiedniego poziomu ochrony danych użytkowników, staje się coraz większym wyzwaniem. Wraz z rozwojem technologii rośnie także liczba zagrożeń związanych z korzystaniem z sieci. Obecnie oprócz szerokiej gamy złośliwego oprogramowania i rozmaitych rodzajów ataków sieciowych należy zwrócić uwagę na znaczącą podatność użytkowników na ataki socjotechniczne. Jednoznacznie można stwierdzić, że

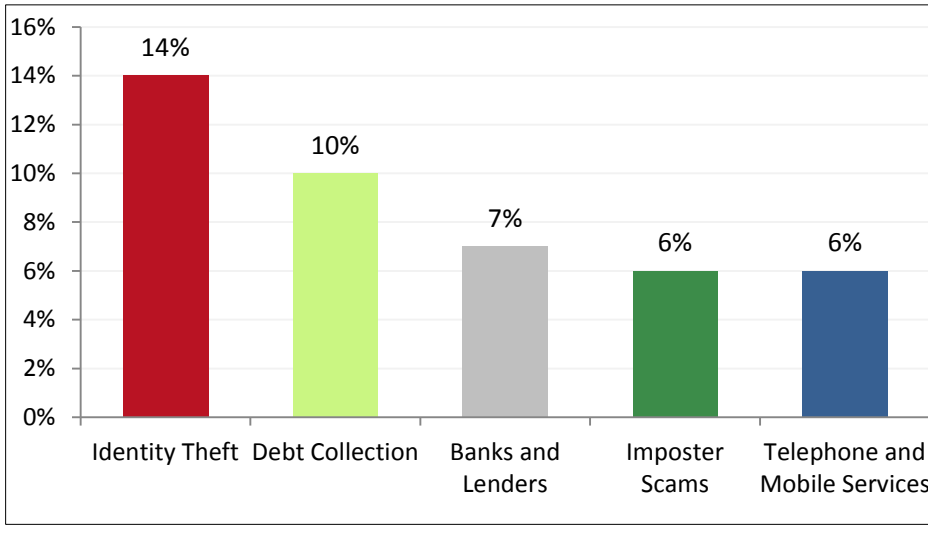
socjotechnika to najniebezpieczniejsza forma ataków na bezpieczeństwo z racji swojej natury. Ponieważ socjotechnika nadużywa cech ludzkich, np. zaufania, nie ma możliwości obrony przed nią tylko i wyłącznie za pomocą hardware'u i software'u. Natomiast uwzględniając ilość zagrożeń i mnogość ich rodzajów, w celu zapewnienia bezpieczeństwa należy zapewnić kompleksową, wielopoziomową ochronę użytkowników. Pierwszy z tych poziomów powinna stanowić odpowiednia edukacja realizowana w wieku wczesnoszkolnym, ze szczególnym naciskiem na edukację w zakresie ochrony tożsamości i ochrony danych osobowych.

Kradzież tożsamości

Każdego roku różne organizacje publikują raporty, z których wynika, że niebezpieczeństwo kradzieży tożsamości obecnie staje się jednym z najpoważniejszych zagrożeń związanych z naszą aktywnością w sieci.

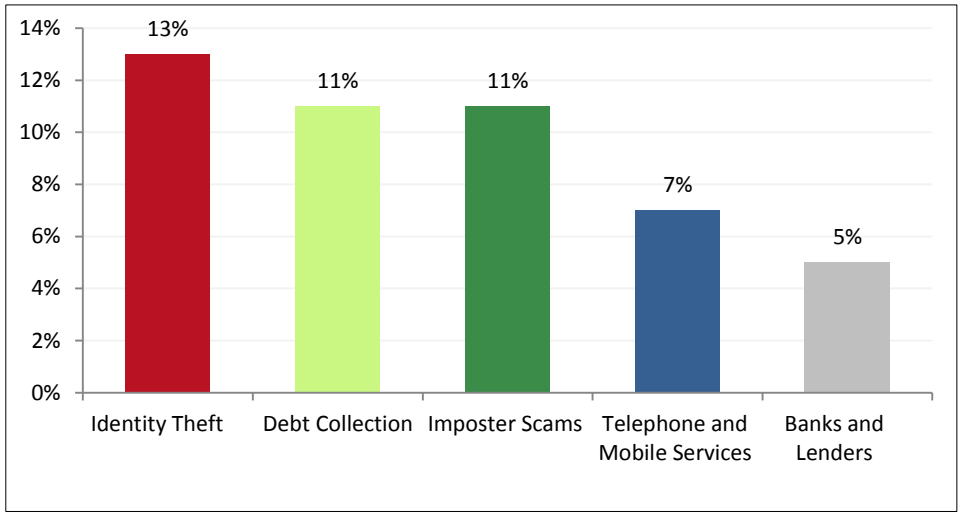
Według rocznego raportu z działalności CERT Polska w 2016 r. zanotowano znaczący wzrost liczby incydentów dotyczących kradzieży tożsamości (o 106% w stosunku do 2015 r.) (CERT Polska, 2017, s. 12).

Analizując statystyki Federalnej Komisji Handlu dotyczące najpopularniejszych w danym roku przedmiotów skarg konsumenckich, wynika, iż kradzież tożsamości od kilku lat utrzymuje się na liście głównych problemów społeczeństwa informacyjnego.



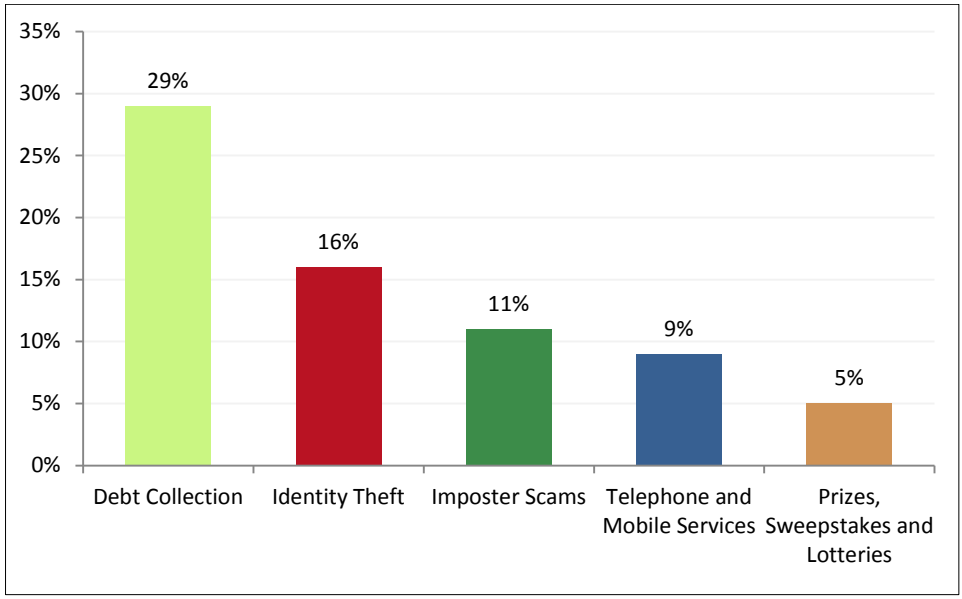
Rysunek 1. Pięć najpopularniejszych przyczyn skarg konsumenckich w Stanach Zjednoczonych w 2013 r.

Źródło: https://www.ftc.gov/news-events/press-releases/2014/02/ftc-announces-top-national--consumer-complaints-2013.



Rysunek 2. Pięć najpopularniejszych przyczyn skarg konsumenckich w Stanach Zjednoczonych w 2014 r.

Źródło: https://www.ftc.gov/news-events/press-releases/2015/02/identity-theft-tops-ftcs-consumer--complaint-categories-again-2014.

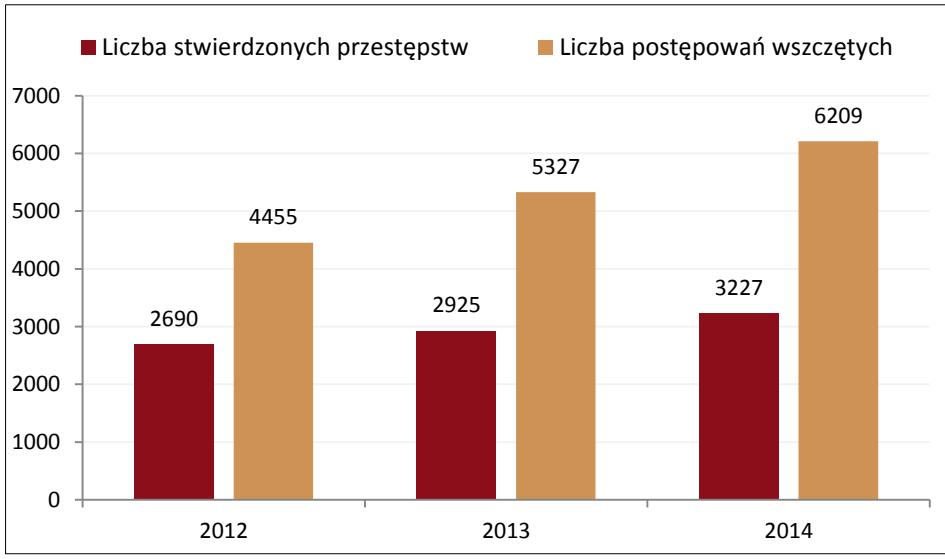


Rysunek 3. Pięć najpopularniejszych przyczyn skarg konsumenckich w Stanach Zjednoczonych w 2015 r.

Źródło: https://www.ftc.gov/news-events/press-releases/2016/03/ftc-releases-annual-summary--consumer-complaints.

Według polskiego prawa kradzież tożsamości jest przestępstwem od 2011 r. Zgodnie z art. 190a § 1 oraz § 2 k.k. „[k]to przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności do lat 3. Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej". Wynika z tego, iż kradzież tożsamości posiada niejako dwa etapy. Najpierw sprawca kradnie dane osobowe, a następnie używa ich, aby popełnić oszustwo, podszywając się pod ofiarę. Fakt, iż proces ten przebiega w dwóch etapach, pociąga za sobą konieczność ochrony użytkowników na dwóch poziomach. Należy nie tylko dołożyć wszelkich starań, by zapobiec kradzieży tożsamości, a także posiąść wiedzę, jak możliwie szybko wykryć kradzież tożsamości oraz jakich narzędzi użyć, by zminimalizować potencjalne szkody.

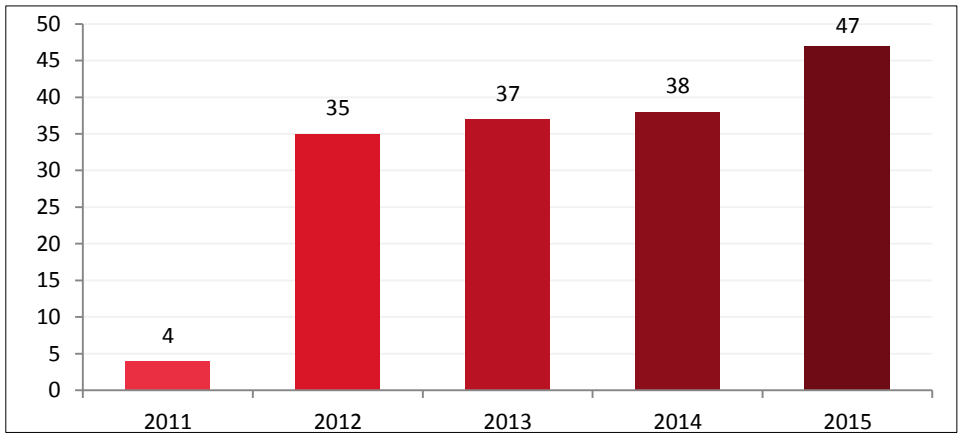
Jak widać na rysunku 4, liczba wykrytych przestępstw związanych z naruszaniem bezpieczeństwa użytkowników w sieci rośnie z roku na rok. Należy również brać pod uwagę, że w rzeczywistości przypadków tych jest znacznie więcej, nie wszystkie są jednak zgłaszane organom ścigania.



Rysunek 4. Statystyka dotycząca przestępstw wszczętych z art. 190a k.k. w latach 2012–2104

Źródło: http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-4/63486,Zmuszanie--art-191.html.

Na rysunku 5 przedstawiono liczbę osób skazanych na podstawie art. 190a § 2 k.k. na przestrzeni ostatnich lat.



Rysunek 5. Liczba osób dorosłych prawomocnie skazanych na podstawie art. 190a § 2 k.k. w latach 2011–2015

Źródło: Informator Statystyczny Wymiaru Sprawiedliwości (2016).

Rosnąca liczba skazanych za przestępstwa związane z kradzieżą tożsamości może świadczyć o narastającym wśród społeczeństwa polskiego problemie niedostatecznej edukacji z dziedziny ochrony tożsamości.

Ochrona tożsamości

Rada ds. Informatyzacji Edukacji (2005) przy Ministrze Edukacji Narodowej podkreśla korzyści płynące z nauki programowania już od najmłodszych lat, jednak równie istotne powinno być nauczanie z zakresu ochrony danych i bezpieczeństwa informacji. Publikowanie informacji o sobie w sieci często staje się powielane i bezrefleksyjne, szczególnie wśród młodych użytkowników portali społecznościowych.

Edukacja z zakresu ochrony tożsamości w sieci powinna uwzględniać różne metody zapewniania jej bezpieczeństwa. Pierwszą z nich jest stosowanie określonych praktyk, które są w stanie znacznie zwiększyć bezpieczeństwo użytkowników sieci, a co za tym idzie – zmniejszyć ich podatność na ataki sieciowe, w tym na te związane z kradzieżą tożsamości. Do praktyk tych należą takie działania, jak: tworzenie bezpiecznych haseł, korzystanie z uwierzytelniania wieloskładnikowego, szyfrowanie danych (zarówno nośników pamięci, jak i poczty elektronicznej), okresowe likwidowanie plików cookies z przeglądarki czy wyłączenie funkcji geolokalizacji w smartfonie. Drugą metodą jest stosowanie odpowiedniego oprogramowania. Rosnąca liczba przypadków kradzieży tożsamości powoduje, iż na rynku oprogramowania powstaje coraz więcej rozwiązań z zakresu ochrony przez kradzieżą tożsamości oferujących m.in. monitorowanie danych osobowych i kont. Także programy antywirusowe nie służą już jedynie wykrywaniu i neutralizowaniu złośliwego oprogramowania. Coraz częściej po-

siadają one również liczne dodatkowe funkcje wykorzystujące analizę behawioralną czy biometrię. Jednym z przykładów takiego oprogramowania jest McAfee – Intel Security True Key, który zapewnia funkcję menedżera tożsamości – True Key. Aplikacja ta chroni hasła, zabezpieczając je za pomocą szyfru AES-256. Zapewnia też uwierzytelnianie wieloskładnikowe np. za pomocą funkcji rozpoznawania twarzy i linii papilarnych, a także zabezpieczenia antyspamowe, w tym ochronę przed phishingiem. Ostatnią metodą jest wykorzystanie fizycznych środków ochrony tożsamości, takich jak filtry prywatyzujące czy czytniki biometryczne, które coraz częściej możemy spotkać w komputerach przenośnych czy smatfonach. Dodatkowo należy zwrócić uwagę na edukację w zakresie działań w wypadku wykrycia kradzieży tożsamości.

Podsumowanie

Obecnie nowe pokolenia dorastają w otoczeniu cyfrowego świata, często nie zdając sobie sprawy z ilości zagrożeń płynących z korzystania z internetu, podczas gdy według GIODO (2016, s. 16) „zjawisko popełniania przestępstw związanych z kradzieżą tożsamości ma charakter niezwykle dynamiczny i stale rośnie, powodując wymierne straty". Zatem aby zapewnić bezpieczeństwo użytkownikom sieci, już na etapie wczesnoszkolnym należy zwrócić szczególną uwagę na edukację w zakresie bezpieczeństwa w cyberprzestrzeni.

Literatura

CERT Polska (2017). *Krajobraz bezpieczeństwa polskiego Internetu w 2016 roku*. Warszawa.

GIODO (2016). *Raport o ochronie danych osobowych*. Warszawa.

Informator Statystyczny Wymiaru Sprawiedliwości (2016). *Skazania prawomocne – stalking – art. 190a kk w latach 2011–2015*. Warszawa: Wydział Statystycznej Informacji Zarządczej Departamentu Strategii i Funduszy Europejskich Ministerstwa Sprawiedliwości.

Lach, A. (2012). Kradzież tożsamości. *Prokuratura i Prawo, 3*, 35–44.

Rada ds. Informatyzacji Edukacji (2015). *Powszechne kształcenie informatyczne w polskim systemie edukacji*. Warszawa: Ministerstwo Edukacji Narodowej.

Ustawa z 6.06.1997 – Kodeks karny. Dz.U. 1997, nr 88, poz. 553, z późn. zm.