Bądź bezpieczny w cyfrowym świecie

Poradnik bezpieczeństwa IT dla każdego

Marcin Pieleszek

onepress Helion

Redaktor prowadzący: Barbara Gancarz-Wójcicka
Recenzja naukowa: dr hab. Agnieszka Dejnaka, prof. WSB.
Projekt okładki: Dominika Zakrzewska (Zakrzewska.art)

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *onepress@onepress.pl*
WWW: *http://onepress.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://onepress.pl/user/opinie?pobeit
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-4589-8

Printed in Poland.

Spis treści

Rozdział 3.

Korzystanie z poczty elektronicznej bez niespodzianek, czyli może nie każdy list jest do Ciebie…

Czy każdy list, który dociera do Twojej skrzynki e-mail, jest do Ciebie? Czy poczta elektroniczna może być źródłem problemów? Pytania te zadaję być może nieco prowokacyjnie.

Zdaniem specjalistów zajmujących się jednym z aspektów ochrony poczty 90%[1] ataków na organizacje zaczyna się od wiadomości mailowej, 50% z nich jest skierowane do mniejszych podmiotów (czyli dotyczy to każdego z nas, nie tylko firm). Liczby robią wrażenie, ale ktoś może powiedzieć, że to przesada i że specjaliści po prostu chcą sprzedać swoje rozwiązania służące do ochrony poczty. Jednak nikt nie może stwierdzić, że problemu nie ma. Ale po kolei.

Zapoznajmy się z kilkoma pojęciami:

Spam — niechciana korespondencja wysyłana masowo (głównie przez mechanizmy automatyczne) na tysiące adresów mailowych. Dlatego nie każda wiadomość jest do Ciebie. Dawniej spam częściej zawierał niechciane oferty handlowe, później zaczął przybierać o wiele groźniejsze formy, takie jak phishing czy załączniki zawierające szkodliwe oprogramowanie (wirusy).

Phishing — podszywanie się (często za pośrednictwem poczty elektronicznej) w internecie pod inną osobę czy instytucję w celu wyłudzenia określonych danych, informacji itp.

Scam — oszustwo polegające na przedstawieniu szlachetnych intencji, np. chęci niesienia pomocy, przekazania atrakcyjnych nagród, przydatnych narzędzi do instalacji na komputerze lub smartfonie, w celu np. dokonania wyłudzeń. Oszustwo to często ma na celu doprowadzenie

[1] Źródło: Cofense.com (dawniej Phishme.com) — amerykańska firma oferująca aktywne wykrywanie zagrożeń płynących z poczty elektronicznej, *https://cofense.com/free/* (dostęp: 7.05.2018).

do tego, by użytkownik (ofiara) nieświadomie uruchomił szkodliwy kod (wirusa) na swoim urządzeniu.

Ransom — okup; cyfrowi przestępcy doprowadzają do uruchomienia na urządzeniu ofiary szkodliwego oprogramowania (ransomware), które szyfruje dane, w wyniku czego użytkownik traci do nich dostęp, po czym otrzymuje od przestępców propozycję odzyskania dostępu po zapłaceniu okupu, zwykle w kryptowalucie (np. bitcoinach).

Przestępcy internetowi (zwani hakerami) wykorzystują prostą socjotechnikę. „Prostą" to nie znaczy nieskuteczną — gdyby te mechanizmy nie działały, nikt nie traciłby czasu na konfigurowanie oprogramowania, które wysyła wiadomości tysiącom użytkowników poczty na świecie. Jakie korzyści mogą płynąć z takich kampanii? W wielkim skrócie — chodzi o sprowokowanie uruchomienia szkodliwego oprogramowania na komputerze ofiary, które będzie miało wpływ na dane. Oprogramowanie może szpiegować zachowania użytkownika, przechwytywać dane z klawiatury, uzyskać kontrolę nad urządzeniami w komputerze, np. nad kamerą, doprowadzić do wycieku danych na serwery przestępców, wreszcie szyfrować dane.

List, w którym przestępca się pod kogoś podszywa, zawiera swoiste „call to action" — wezwanie do akcji. Użytkownik, śpiesząc się w trakcie wykonywania swojej pracy, nie zwraca uwagi na szczegóły otrzymywanej korespondencji, chce np. szybko wyjaśnić sprawę — klika i uruchamia szkodliwy mechanizm. Emocje, pośpiech i ciekawość są w tym przypadku bardzo złymi doradcami. Przekaz wzywający nas do szybkiej i emocjonalnej reakcji to dość skuteczna metoda, która może prowadzić do tego, że użytkownik kliknie link w wiadomości odwołujący się do strony z wirusem lub otworzy załącznik zawierający szkodliwe oprogramowanie. Przed problemami może nas uchronić uważne przeczytanie takiej wiadomości bez żadnej dalszej reakcji lub jej skasowanie.

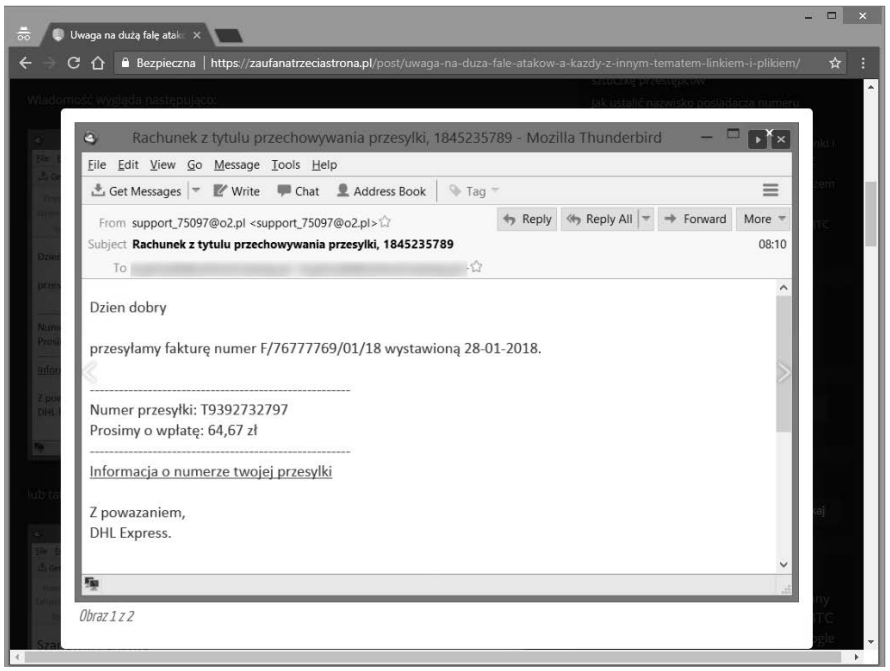
Aby ustrzec się przed takimi sytuacjami, powinniśmy znać zwyczaje przestępców i wiedzieć, pod kogo mogą się podszywać. Taka świadomość w dużym stopniu może chronić przed problemami. Ale przedstawienie pełnej listy sytuacji niebezpiecznych z przykładami nie jest możliwe. Zagrożenia cały czas się zmieniają. Dlatego przedstawię tu katalog tylko najpowszechniej występujących zagrożeń. Pomogą w tym przykłady z serwisu poświęconego bezpieczeństwu technologicznemu Zaufana Trzecia Strona.

3.1. Firmy kurierskie

Otrzymujesz maila z informacją typu „opłać przesyłkę", „nie odebrałeś przesyłki" lub „nie odebrałeś kilku przesyłek" — i od razu działasz. Tymczasem trzeba się zastanowić, czy faktycznie spodziewamy się przesyłki, czy wiadomość wygląda tak jak zwykle, czy jest wysłana z adresu firmy kurierskiej, czy linki w wiadomościach prowadzą do strony firmy, z której usług zwykle korzystamy, czy numery przesyłki się zgadzają i mają ten sam format co zwykle. Może trzeba sprawdzić kopię listu przewozowego, wejść na stronę firmy logistycznej, wpisać numer przesyłki, aby zobaczyć, co się z nią dzieje. To zdecydowanie najbezpieczniejsza strategia.

Jeśli nie oczekujesz na żadną przesyłkę, to od razu takiego maila zlekceważ i wyrzuć do elektronicznego kosza. Natomiast w firmach działy logistyczne, które przetwarzają dokumenty przewozowe, powinny przejść drobiazgowe wewnętrzne szkolenia, uświadamiające zagrożenia oraz wyraźnie definiujące cechy oryginalnych informacji z firm kurierskich (logistycznych). Trzeba zaznaczyć, że maile przestępców mogą (ale niekoniecznie zawsze tak jest) wiernie naśladować oryginały.

Na rysunku 3.1 widać przykład maila, który został wysłany z innej domeny niż używana przez firmę dostarczającą przesyłki. W takim przypadku podszycie się pod tę firmę jest dość łatwe do zidentyfikowania, pod warunkiem że jesteś czujny. Ale od razu trzeba zaznaczyć, że w pole „mail from" (wiadomość od) przestępca może wpisać adres, którego się spodziewamy (na szczęście nie zawsze zachowuje taką staranność), jeżeli ma skonfigurowany do wysyłki serwer pocztowy, który to zaakceptuje. Wówczas zidentyfikowanie rzeczywistego adresu skrzynki pocztowej, z której wiadomość została wysłana, będzie możliwe tylko w źródle wiadomości, co nie jest już oczywistą i prostą procedurą. Jeżeli masz poważne podejrzenia, a mail wygląda na istotny, zwróć się o pomoc do specjalistów IT lub wyszukaj w internecie informacje na temat tego, jak wyświetlić źródło maila w Microsoft Outlook czy w Thunderbird, i wykonaj diagnozę samodzielnie.



RYSUNEK 3.1. *Przykład podszywania się pod firmę kurierską.*
Źródło: „Uwaga na dużą falę ataków — a każdy z innym tematem, linkiem i plikiem", 8.02.2018, https://zaufanatrzeciastrona.pl/post/uwaga-na-duza-fale-atakow-a-kazdy-z-innym-tematem-linkiem-i-plikiem/ (dostęp: 9.05.2018)

Klient poczty Thunderbird:

- Kliknij raz wiadomość.
- Wybierz z menu *Widok/Źródło wiadomości*.

Klient poczty Microsoft Outlook:

- Kliknij dwa razy sprawdzaną wiadomość, tak aby otworzyła się w nowym oknie.
- Kliknij *Plik/Właściwości* — w polu *Nagłówki internetowe* wyświetli się źródło wiadomości.

Należy zwrócić uwagę, czy w źródle wiadomości wszędzie pojawia się prawidłowa i ta sama domena nadawcy. W serwisach *who.is, ripe.net* możemy również sprawdzić adres IP nadawcy.

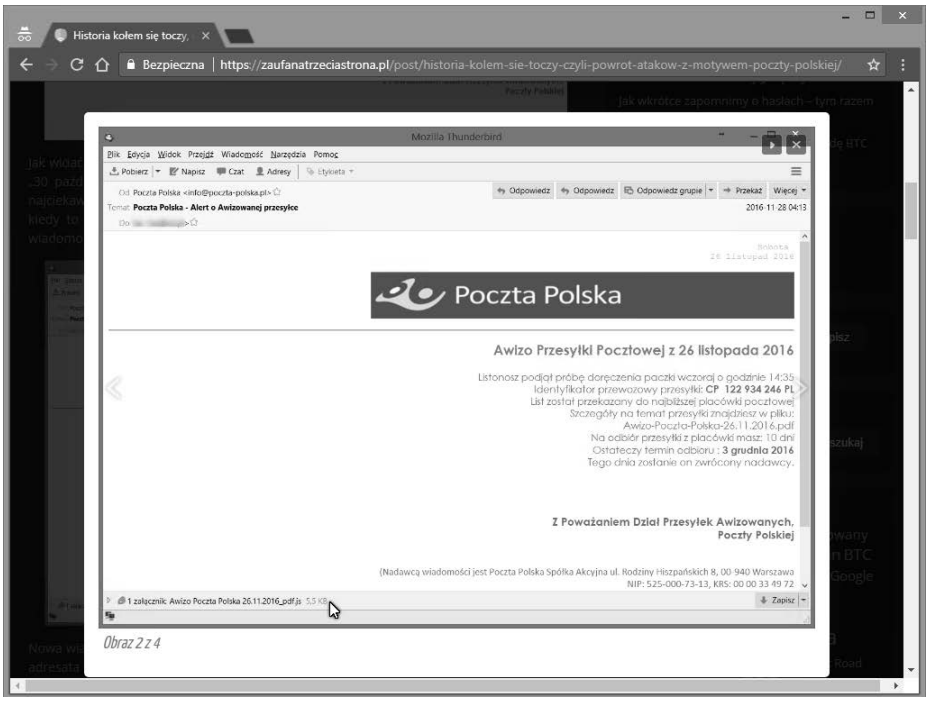
Jeżeli jednak nie spodziewałeś się przesyłki z konkretnej firmy, to taki mail od razu powinien trafić do kosza, bez czytania. Tak przecież często traktujesz niechcianą korespondencję papierową.

Na rysunku 3.2 mamy przykład podszywania się pod Pocztę Polską, tym razem na pierwszy rzut oka trudniej jest nabrać podejrzeń. Ewidentne wątpliwości budzi załącznik, gdyż nie ma rozszerzenia **.pdf* (dokumentu elektronicznego), tylko **.js* (JavaScript — język programowania). Kod uruchamiał szyfrowanie danych. Mylące potencjalną ofiarę jest to, że litery „pdf" są częścią nazwy pliku. Prościej jest skasować maila, którego się nie spodziewaliśmy.

3.2. Faktury i rachunki od dostawców usług telekomunikacyjnych, energii elektrycznej itp.

Ofiarami ataku mogą stać się klienci różnych firm korzystający z szerokiej palety usług i rozliczający się za nie. Ogólnie określam to zwykle tak, że przestępcy podszywają się pod dostawców „usług wszelakich". Przejdźmy jednak do konkretów. Firmy z sektora finansowego wysyłają powiadomienia o wystawionych fakturach, np. za usługi leasingu. Zwykle maile od instytucji finansowych zawierają tylko powiadomienie o wystawionej fakturze, a sam dokument pobiera się z serwisu do tego przeznaczonego po samodzielnym wejściu na adres WWW i zalogowaniu się. W wiadomości nie ma zwykle żadnego linku do logowania (np. do serwisu obsługi klienta, a tym bardziej bankowości internetowej). Trochę mniej wygodne, ale bezpieczne.

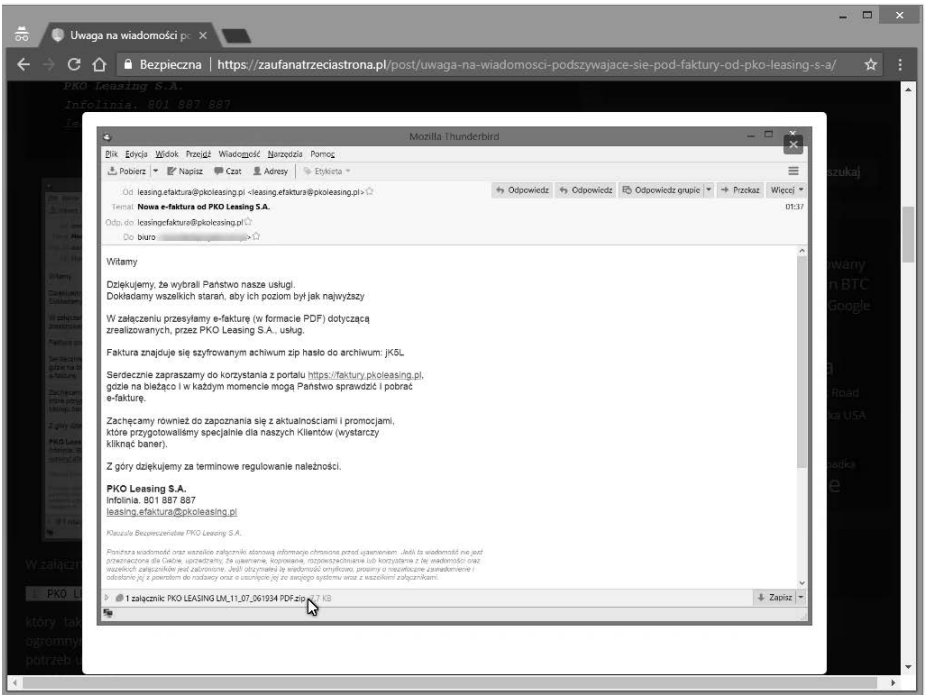
Przestępcy postępują oczywiście inaczej i powinno to budzić zawsze nasze wątpliwości. Na rysunku 3.3 pole *Od* na pierwszy rzut oka wskazuje na bank, ale link w mailu niekoniecznie jest bezpieczny; największe wątpliwości od razu powinien wzbudzić sposób otwierania załącznika **.zip* z hasłem. Właśnie tak szkodliwe oprogramowanie (wirus) próbuje ominąć mechanizmy antyspamowe, które nie mogą od razu przeskanować takiego załącznika i w przypadku braku radykalnych zabezpieczeń mogą go przepuścić do naszej skrzynki,



RYSUNEK 3.2. *Przykład podszywania się pod Pocztę Polską.*
Źródło: „Historia kołem się toczy, czyli powrót ataków z motywem Poczty Polskiej", 20.10.2017, https://zaufanatrzeciastrona.pl/post/historia-kolem-sie-toczy-czyli-powrot-atakow-z-motywem--poczty-polskiej/ (dostęp: 9.05.2018)

kwalifikując go ewentualnie jako spam. Następnie użytkownik decyduje, co w folderze *Spam* uzna za przydatną wiadomość — nieco niefrasobliwa osoba może próbować otwierać załącznik, klikać link itd. Oczywiście nazwa pliku zawiera dla zmylenia trzy litery „pdf" (wskazujące tylko pozornie na dokument elektroniczny), ale nie jest rozszerzeniem pliku **.pdf*. W tym przypadku w skompresowanym pliku występował skrypt **.js* (JavaScript) ze szkodliwym programem, umożliwiającym przejęcie kontroli nad komputerem ofiary.

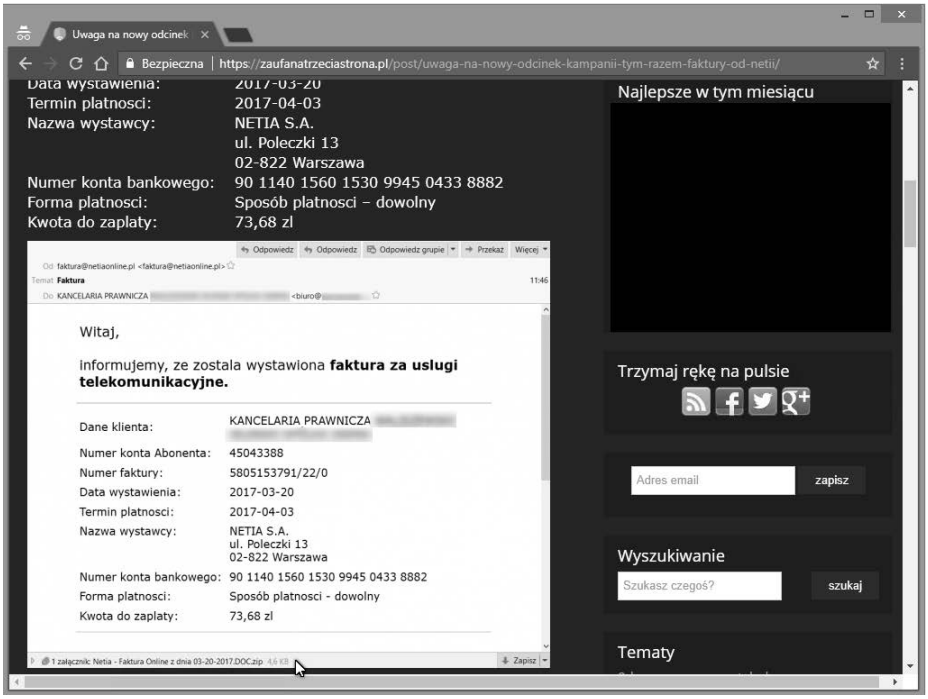
Podobny przykład podszywania się, ale już pod firmę z innej branży, przedstawia rysunek 3.4. Dość często zdarzają się ataki polegające na udawaniu firmy z branży telekomunikacyjnej. Wynika to z tego, że te podmioty, aby ułatwiać klientom rozliczenie za usługi, wysyłają faktury e-mailem, w pliku PDF. W każdym przypadku bezpieczną praktyką będzie samodzielne wejście na stronę i po sprawdzeniu, czy ze stroną jest wszystko w porządku (o czym będę pisał w kolejnych rozdziałach), zalogowanie się do serwisu swojego operatora i samodzielne pobranie faktury. Budując strategię firmową informowania klienta o wystawionych dokumentach, być może warto pomyśleć w taki sposób, aby mail był tylko informacją o wystawionych w portalu klienta dokumentach.



RYSUNEK 3.3. *Przykład podszywania się pod bank.*
Źródło: „Uwaga na wiadomości podszywające się pod faktury od PKO Leasing S.A.", 12.07.2017, https://zaufanatrzeciastrona.pl/post/uwaga-na--wiadomosci-podszywajace-sie-pod-faktury-od--pko-leasing-s-a/ (dostęp: 9.05.2018)

W podanym przykładzie pole *Od* także wydaje się wskazywać dostawcę usług. Ważny jest oczywiście kontekst — czy spodziewaliśmy się faktury, czy korzystamy z usług danej firmy, czy obsługujemy w swojej firmie faktury itp. Ale wątpliwości budzi ponownie załącznik. Udaje on plik edytora tekstu Word z rozszerzeniem **.doc*, ale jest plikiem skompresowanym ZIP (**.zip*). Tym razem można było znaleźć w mailu hasło do pliku i po wielu kliknięciach (co powinno wzbudzić podejrzenia) uruchomić szkodliwe oprogramowanie.

Szczególną ostrożność należy zachować przy korzystaniu z usług finansowych. Nigdy nie wolno logować się do banku poprzez link w mailu — o tym będzie jeszcze mowa w kolejnych rozdziałach. Maksymalna ostrożność jest również wymagana przy korzystaniu z systemów płatności internetowych. Pod systemy płatności internetowych również podszywają się przestępcy. Na rysunku 3.5 pokazano przykład rzekomego potwierdzenia płatności przez internet — tu znowu pojawia się załącznik. Schemat podobny do poprzednich — załącznik udaje plik w formacie Worda (**.doc*), a tak naprawdę jest to plik archiwum, w którym



RYSUNEK 3.4. *Przykład podszywania się pod dostawcę usług telekomunikacyjnych. Źródło: „Uwaga na nowy odcinek kampanii, tym razem »Faktury od Netii«", 20.03.2017, https://zaufanatrzeciastrona.pl/post/uwaga-na-nowy-odcinek-kampanii-tym-razem-faktury-od-netii/ (dostęp: 9.05.2018)*

znajduje się szkodliwy skrypt (program) JavaScript (**.js*). Kliknięcie tego pliku uruchamiało program (skrypt) w PowerShell[2] i rozpoczynało szyfrowanie dysku.

Rysunek 3.6 przedstawia witrynę przestępców, która otwiera się po kliknięciu linku do strony WWW w mailu z rzekomym rachunkiem za energię elektryczną. Należy zwrócić uwagę na kilka ważnych rzeczy. W wierszu adresu przeglądarki domena *pge-bok14.org* nie jest prawidłową domeną internetową używaną przez dostawcę energii elektrycznej. Plik ze szkodliwym kodem JavaScript (**.js*) tym razem nie jest w załączniku wiadomości mailowej, tylko jest pobierany ze strony. Kolejny złodziejski sposób na ominięcie zabezpieczeń antyspamowych. Po uruchomieniu kodu uruchamiał się program ransomware przedstawiający się jako *Crypt0L0cker*, a złodziejska stawka za odszyfrowanie plików wynosiła ponad tysiąc złotych w kryptowalucie.

[2] PowerShell — środowisko pozwalające na uruchomienie poleceń do konfigurowania systemów Microsoft Windows i administrowania nimi. Uruchomione z prawami administratora daje pełną kontrolę nad systemem.

Skorowidz

R

S

T

U

V

W

Z

(Ni)e-bezpieczeństwo?

Większość z nas nie wyobraża sobie dnia bez internetu. Dostęp do informacji, kontakt ze znajomymi, zakupy w sieci, przelewy online, wirtualna edukacja... Nowy, wspaniały świat wszechobecnej technologii, która oferuje nieograniczone możliwości. Niestety, w świecie tym obecni są nie tylko ludzie prawi. Sieć, a wraz z nią my sami, coraz częściej pada ofiarą nieuczciwych członków cyfrowej społeczności. Z miesiąca na miesiąc rośnie liczba przestępstw popełnianych w internecie. Pojawiają się programy, które paraliżują całe firmy, organizacje, instytucje, narażając je na bardzo dotkliwe straty. Zwykli ludzie tracą pieniądze jako ofiary wyłudzeń lub po prostu włamań na konta bankowe.

Nasze cyfrowe bezpieczeństwo w znacznej mierze zależy od nas samych. To użytkownik technologii powinien uważać na swoje zachowania w wirtualnym świecie. A ten jest przyjazny, pod warunkiem że przestrzega się pewnych zasad. O tym, jakie to zasady, mówi ta książka. Napisana przez zawodowego informatyka przystępnym, zrozumiałym językiem, jest skierowana do każdego, kto korzysta z internetu w pracy i poza nią — słuchając muzyki, rozmawiając ze znajomym na czacie czy szukając przepisu na ciasto. Poza wiedzą teoretyczną poradnik wskazuje praktyczne narzędzia — zwykle darmowe — dzięki którym można szybko podnieść poziom swojego cyfrowego bezpieczeństwa. Przeznaczone są one dla powszechnie używanych systemów: Windowsa na komputerze i Androida na urządzeniu mobilnym.

Helion
onepress
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

ISBN 978-83-283-4589-8