Alicja Żarowska-Mazur

Cyfrowy świat seniora

Bezpiecznie w internecie

PWN

Projekt okładki i stron tytułowych **Sebastian Machulik**

Ilustracja na okładce **Shutterstock/Andrey_Popov**

Wydawca **Łukasz Łopuszański**

Redaktor prowadzący **Jolanta Kowalczuk**

Koordynator produkcji **Anna Bączkowska**

Skład i łamanie **INT-MEDIA Dawid Mazur**

ISBN 978-83-01-18561-9

Wydanie I
Warszawa 2016

Wydawnictwo Naukowe PWN SA
02-460 Warszawa, ul. Gottlieba Daimlera 2
tel. 22 69 54 321, faks 22 69 54 288
infolinia 801 33 33 88
e-mail: pwn@pwn.com.pl
www.pwn.pl

Informacje w sprawie współpracy reklamowej: reklama@pwn.pl

Druk i oprawa: **Drogowiec-PL**

Spis treści

WSTĘP

Bezpieczeństwo w sieci zazwyczaj kojarzy się z atakami hakerskimi. Tymczasem bezpieczeństwo to nie tylko cyberprzestępczość. To wykorzystanie internetu w bardziej przyziemnych celach: sprzedanie wadliwego produktu, wypromowanie marki kosztem innej, zachęcenie użytkownika do popełnienia czynów, których sam by się nie dopuścił, ponieważ nie pozwala mu na to jego uczciwość.

Dzięki tej książce zobaczysz, że w internecie, mimo wszystkich jego pozytywnych stron, czyha także wiele pułapek. Czasem myślimy, że dotyczą one głównie dzieci i młodzieży. Okazuje się jednak, że również osoby dorosłe nie zawsze są w stanie ustrzec się przed wszystkim. Zamiast więc wpadać w megalomanię, warto się pochylić przez chwilę nad tym, co nam grozi, jeśli nie będziemy ostrożni.

Pamiętaj, że książka ta ma cię przestrzec, lecz nie zrazić do korzystania z sieci. W obecnych czasach trudno bowiem egzystować bez internetu. To w nim na bieżąco możesz śledzić informacje, które w pozostałych mediach pojawiają się nieraz z kilkudniowym opóźnieniem. To dzięki internetowi dokonujesz szybkich zakupów i równie szybko płacisz za towary i usługi. Grunt to uważać i nie otwierać się przed nieznajomymi użytkownikami, tak jak robimy to w gronie przyjaciół. Nigdy nie wiemy, kto czyta nasze wypowiedzi i śledzi wpisy, gdzie akurat jesteśmy.

Krótko mówiąc, od dziś niech ostrożność będzie twoim drugim imieniem, a nic ci nie będzie grozić. Powodzenia!

1. NIE DAJ SIĘ HAKEROM

W poprzednich książkach z serii *Cyfrowy świat* wielokrotnie zwracałam uwagę na temat bezpieczeństwa. Pochylmy się nad tą kwestią nieco bardziej. Myśląc o bezpieczeństwie w sieci, często bowiem nie zdajemy sobie sprawy, że tak naprawdę zabezpieczenie danych to nie tylko zainstalowanie właściwego oprogramowania, lecz również wzmożona czujność w takich miejscach, jak bankomaty czy centra handlowe. Zobaczmy, z jakimi zagrożeniami możesz się zetknąć, jak na nie reagować, a przede wszystkim, jak się zabezpieczać.

Cyberprzestrzeń (**przestrzeń cybernetyczna** lub **przestrzeń informatyczna**) to przestrzeń, w której komunikują się ze sobą urządzenia, takie jak komputery, laptopy, tablety, smartfony, terminale itp.

Jeżeli czytasz tę książkę, to zapewne korzystasz z komputera, smartfonu czy tabletu. Jesteś więc aktywnym uczestnikiem cyberprzestrzeni. Oprócz uczciwych ludzi w przestrzeni tej działają oczywiście przestępcy zwani cyberprzestępcami.

Co może zrobić taki cyberprzestępca? Wszystko to, co zwykły przestępca, lecz za pomocą dostępnych środków informatycznych. Można się zatem spodziewać kradzieży, oszustw, wyłudzania informacji, podszywania się pod nas, wykorzystania naszych danych.

1.1. Hacking

Najbardziej znanym przestępstwem, z jakim mamy do czynienia w cyberprzestrzeni, jest **hacking**, czyli nieautoryzowany dostęp do danych umieszczonych w sieci lub systemie. Pojawił się on na tyle wcześnie, że doczekał się już wielu filmów na swój temat. Co prawda, tam hacking jest przedstawiany spektakularnie, niemal magicznie. Tymczasem w rzeczywistości hakerzy działają po cichu, lecz bardzo skutecznie.

Czy ten osobnik z naprzeciwka nie jest przypadkiem hakerem? Być może jest. Ale tylko pod warunkiem, że to programista lub pasjonat o bardzo rozległej wiedzy informatycznej. Obecnie komputery są zabezpieczane na podstawowym poziomie już podczas instalacji systemu operacyjnego. Dla przeciętnego

użytkownika już takie zabezpieczenie jest raczej nie do obejścia. Łamanie zabezpieczeń sieci i systemów komputerowych wymaga zdecydowanie większych umiejętności.

Czy hacking może dotyczyć cię osobiście? Tak. To najczęściej wyjątkowa złośliwość kogoś, kto dowiedział się, jak sobie poradzić z zabezpieczeniami i buszuje po przypadkowych komputerach. Najczęściej jednak hakerzy atakują komputery i strony rządowe, różnych organizacji oraz korporacji. Czasami ataki hakerskie mają na celu jedynie wskazanie właścicielom lub administratorom luk w zabezpieczeniach, a nie wykradzenie informacji. Można więc powiedzieć, że nie każdy haker jest z gruntu zły i niekoniecznie musi być cyberprzestępcą. Niezależnie od tego, jaki hacking może cię dotyczyć, komputer powinien być przed nim należycie zabezpieczony. Przede wszystkim nie wyłączaj zabezpieczeń systemowych, takich jak zapora sieciowa.

No tak… Luka, zabezpieczenia, zapora. Wszystko fajnie, ale co to wszystko w praktyce oznacza? Mniej więcej to, że system komputerowy jest bardzo złożonym programem, który składa się z wielu mniejszych programów. Przy tak ogromnych projektach pracuje oczywiście wielu programistów, ale również analityków i testerów. Przeprowadza się wiele testów oprogramowania, które mają wykazać ewentualne błędy. Znalezienie jednak wszystkich graniczy niemal z cudem.

Hakerzy skupiają się głównie na znalezieniu błędów i za pomocą takich luk są w stanie włamać się do systemu, tak jak złodziej włamuje się do niewłaściwie zabezpieczonego domu czy sklepu. Złodziej może cię okraść, ale może też narazić cię na zniszczenia mebli, sprzętów, pomieszczeń. Hakerzy natomiast mogą wpuścić do twojego systemu szkodliwe oprogramowanie, które również może wpłynąć negatywnie na funkcjonowanie systemu lub pozwoli na regularne pozyskiwanie danych.

1.2. Cracking

Wiele osób, nieraz nieświadomie, uczestniczy w **crackingu**. Jego celem także jest łamanie zabezpieczeń, jednak dotyczy on dwóch różnych dziedzin: sieci komputerowych i oprogramowania. Pamiętaj, że cracking to łamanie prawa

i jeżeli zostaniesz na nim złapany, to nikt nie będzie cię pytał, czy wiedziałeś, co robisz, i czy miałeś świadomość, że działasz niezgodnie z prawem. I zgodnie ze starą prawdą: nieznajomość prawa szkodzi. Tak jest też w tym przypadku.

Cracking sieciowy często jest utożsamiany z hackingiem. Najczęstszym obiektem działań crackerów są firmy i organizacje mające złą opinię społeczną. Crackerzy mogą ukrywać swoją obecność i zapewniać sobie możliwość ponownego dostępu do zasobów przez uchylenie tylnych drzwi. Takie drzwi, zwane też furtką, to specjalna luka (ang. *backdoor*), przez którą przemykają niepostrzeżenie w dowolnym czasie. Ale co ty masz z tym wspólnego? Jeszcze nic. Dopiero drugi rodzaj crackingu to z pewnością znane ci, nawet jeśli nie z autopsji, to na pewno ze słyszenia, działania dotyczące oprogramowania komercyjnego.

Jak zapewne zdążyłeś się już zorientować, ceny oprogramowania często sięgają chmur. Kupując nowy sprzęt, najczęściej w pakiecie otrzymujesz system operacyjny. Pozostałe aplikacje musisz jednak zainstalować samodzielnie. Wśród nich zwykle są pakiety biurowe (głównie edytor tekstu, arkusz kalkulacyjny i program to tworzenia prezentacji multimedialnych), czasami programy graficzne umożliwiające podstawową obróbkę zdjęć lub edytory stron internetowych. Wiele programów ma swoje darmowe odpowiedniki. Należy jednak liczyć się z tym, że o ile główne funkcje są zbieżne z funkcjami oprogramowania komercyjnego, o tyle szczegóły mogą pozostawiać nieco do życzenia. Niemniej nie zmienia to faktu, że tak wysokie koszty oprogramowania komercyjnego stanowią barierę, którą bardzo często ciężko jest pokonać. Wiele osób decyduje się więc na instalację nielegalnego oprogramowania.

Zazwyczaj wymaga to zainstalowania dodatkowego pliku, tzw. cracka, lub użycia generatora kluczy, czyli keygena. Potrafią one wygenerować odpowiednio numer seryjny potrzebny do zarejestrowania oprogramowania oraz numer aktywacyjny, aby użytkownik mógł korzystać z pełnej wersji danego programu. Pamiętaj, że ten sposób nabycia pełnej wersji oprogramowania jest niezgodny z prawem i korzystając z niego, po pierwsze narażasz swój komputer na różnego rodzaju infekcje, po drugie łamiesz prawa autorskie. Mówiąc bardziej dosadnie, po prostu kradniesz, a to, rzecz jasna, jest karalne. Powstaje więc pytanie, czy lepiej skorzystać z tzw. wolnego oprogramowania, które może nie mieć wszystkich funkcji, jednak jest darmowe i możesz go używać bez ograniczeń, czy zastosować cracki i keygeny, a później nie spać po nocach i zastanawiać się, jakie to może przynieść konsekwencje.

Abyś nie musiał się nad tym zastanawiać, rozwiejmy od razu wątpliwości. Oprócz kary umownej zgodnie z Ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (art. 118) należy się liczyć z karą grzywny oraz ograniczenia wolności albo pozbawienia wolności do roku. Jeśli więc wydaje ci się, że zainstalowanie jakiegoś programu to nic takiego – przecież nikt się nie kapnie, to radzę dwa razy się nad tym zastanowić. Komputery komunikują się ze sobą w sieci, oprogramowanie często pobiera aktualizacje z internetu. Ustalenie, że na twoim komputerze znajduje się nielegalne oprogramowanie, jest możliwe i naprawdę nie wymaga wielkiego wysiłku.

Bankomaty to również miejsce, gdzie dość łatwo paść ofiarą przestępstwa. W 2010 roku powstał program Dillinger, za pomocą którego jego twórca udowodnił producentom bankomatów, że co prawda kasety z pieniędzmi mają dość dobre zabezpieczenia i dostanie się do nich nie jest prostą rzeczą, jednak wgranie złośliwego oprogramowania lub zarządzanie bankomatem z zewnętrznego komputera i wysłanie mu komunikatu, aby rozpoczął wypłacanie gotówki, jest niewiarygodnie łatwe. Część producentów od razu załatała dziurę w oprogramowaniu. Należy przypuszczać, że na przełomie kolejnych lat również inni wzięli z nich przykład.

1.3. Skimming

Aspirant Maczek z uwagą oglądał umieszczony nad monitorem nawis reklamowy. Nie miał wątpliwości, że to oryginalny składnik bankomatu. Ale coś tu musiało nie grać – o ile, rzecz jasna, wczorajsza analiza była prawidłowa. Policjant ponownie zbliżył twarz do plastikowej powierzchni. I wtedy na jej dolnej krawędzi dostrzegł połyskującą smugę. Dotknął jej palcem i poczuł lepki opór.

– Klej – mruknął pod nosem. – Normalny klej.

Zrobił kilka fotografii, po czym sięgnął po komórkę i połączył się z nadkomisarzem Pawłowskim.

– Używają kleju, żeby to zamocować – powiedział.

Wniosek był zasadniczo poprawny. Tyle że ani aspirant, ani jego pryncypał nie wiedzieli, czym „to" jest bądź czym może być[1].

[1] *Cyberkryminalni: Skimming po polsku*, `www.chip.pl`.

Obecnie, korzystając z kart płatniczych, jesteśmy raczej narażeni na **skimming**. Przytoczony fragment tekstu odnosi się do pierwszego przypadku skimmingu wykrytego w Europie. Skimming można porównać do skanowania, czyli przebiegowego odczytywania obrazów i różnych kodów. Skaner zna każdy z nas, choć nie zawsze zdaje sobie z tego sprawę. Kiedy sprawdzasz cenę produktu w hipermarkecie za pomocą czytnika, w rzeczywistości skanujesz kod na produkcie. Tak samo jest przy kasie, bardzo często również podczas dostarczania paczek przez firmy kurierskie – za pomocą przenośnych terminali skanuje się kod umieszczony na paczce, dzięki czemu niepotrzebne są stosy papierków, na których potwierdzasz odbiór przesyłki. W przypadku skimmingu odczytywane są informacje zapisane na pasku magnetycznym karty. Służą one przestępcom do tworzenia fałszywych kart. Działają one identycznie jak oryginalne i umożliwiają przeprowadzenie wszystkich operacji kosztem posiadacza oryginału.

Ze skimmingiem możemy spotkać się zarówno w bankomatach, jak i placówkach handlowych oraz usługowych. W przypadku bankomatów wygląda to tak, że są w nich instalowane specjalne urządzenia pozwalające na odczytanie danych. Aby sfałszowana karta była w pełni funkcjonalna, potrzebny jest oczywiście PIN. W tym celu w bankomacie instaluje się kamery, klawiatury, którymi są przykrywane oryginalne klawiatury, lub nakładki na czytniki kart, dzięki którym możliwe jest przechwycenie danych, czyli w tym przypadku kodu PIN (rys. 1).

W drugim przypadku, czyli w placówkach handlowych i usługowych, skimming ma nieco inną formę. Zazwyczaj odpowiedzialność za ten proceder ponoszą osoby, które nas obsługują, np. sprzedawcy, kelnerzy, pracownicy serwisów. Kilkanaście lat temu w wielu restauracjach dość powszechny był brak terminali przenośnych. Czasami klient był proszony o podejście do kasy i uregulowanie rachunku, czasami jednak tylko o udostępnienie karty. Niestety, po sprawdzeniu wyciągu z konta bankowego okazywało się, że klient był uboższy o zdecydowanie wyższą kwotę niż widoczna na rachunku. Były to pojedyncze oszustwa, a klienci dość szybko orientowali się w sytuacji. Przestępcy zdają się tym jednak nie przejmować. Na szczęście klienci są coraz bardziej świadomi, wiedzą, jak dbać o swoje bezpieczeństwo i o swoje pieniądze i coraz rzadziej pozwalają, by ich karta znikała z ich pola widzenia. Pocieszający jest także fakt, że przy tego typu skimmingu przestępcy rzadko mają dostęp do kodu PIN.

O ile w przypadku placówek handlowych lub usługowych podstawową formą zabezpieczenia jest po prostu czujność i świadomość, że karty nie należy spuszczać z oczu, o tyle w sytuacji skimmingu bankomatowego jest już nieco trudniej.

Rysunek 1. Przykład fałszywej klawiatury i nakładki na czytnik kart, źródło: www.europol.europa.eu

Przestępcy nie mają możliwości dostania się do wnętrza bankomatu. Wszystkie urządzenia, którymi się posługują, mają formę nakładek montowanych najczęściej za pomocą kleju. Patrz więc uważnie, czy klawiatura, która zazwyczaj jest wpuszczona w urządzenie, nie wystaje dziwnie wysoko, upewnij się, że kamera jest wewnątrz urządzenia, a nie na zewnątrz i przede wszystkim nie jest skierowana na klawiaturę, sprawdź także, czy czytnik kart nie jest uszkodzony, przekręcony, bo to może oznaczać, że został przytwierdzony tymczasowo. Warto też zobaczyć na stronie internetowej swojego banku, jak wyglądają jego oryginalne bankomaty.

1.4. Zadbaj o pliki

Wiesz już, jakie są podstawowe zagrożenia w cyberprzestrzeni. A jak im zapobiegać? Przede wszystkim należy dbać o porządek w komputerze, telefonie, tablecie.

Pracując w biurze czy na budowie, nie zostawiasz wszystkiego na biurku lub pod nogami, bo:

- możesz się o coś potknąć i przewrócić;
- wiatr może sprzątnąć ci sprzed nosa ważne notatki;
- ktoś może przyjść i wziąć sobie to, czego akurat potrzebuje, a ty zostaniesz bez narzędzi pracy lub ważnego projektu;
- w bałaganie trudno jest znaleźć właściwe rzeczy.

Zapamiętaj!

Socjotechnika (inżynieria społeczna) to działania, metody i środki prowadzące do manipulacji społeczeństwem. Szczególnie wyraźnie takie metody są widoczne w niektórych mediach, zwłaszcza w państwach o systemie totalitarnym.

Komputer, urządzenia mobilne, kartę płatniczą również powinieneś zabezpieczyć – i przed bezpośrednim dostępem niepowołanych osób, i przed dostępem z zewnątrz.

W jaki sposób hakerzy i crackerzy mogą dostać się do komputera? Sposobów jest bardzo wiele. Pierwszy, o którym większość z nas nie myśli, ponieważ zazwyczaj ufamy swojej rodzinie i znajomym, to użycie pamięci przenośnych.

Pamięci przenośne to np. pendrive'y lub dyski zewnętrzne. Na pewno kojarzysz takie sceny z filmów sensacyjnych – ktoś zostaje na chwilę sam w pomieszczeniu i rozglądając się nerwowo, wsuwa kartę lub pendrive'a do komputera, po czym kopiuje setki plików lub niszczy je i zachowując twarz pokerzysty, wychodzi. Możliwe tylko w filmach? Okazuje się, że jednak nie. Może wyszukanie i skopiowanie takiej ilości materiałów jest nieco naciągnięte, jednak sam mechanizm jest rzeczywisty. Wystarczy na kilka sekund umieścić pamięć przenośną w komputerze, żeby znalazło się w nim oprogramowanie pozwalające na zbieranie informacji lub wirus, który zainfekuje komputer.

Jeżeli sam musisz użyć cudzego nośnika USB, to przeskanuj go najpierw pod kątem ewentualnych wirusów. Często zdarza się, że przy okazji szkoleń, konferencji, spotkań integracyjnych itp. dostajesz różne gadżety, między innymi właśnie pamięci przenośne. Oczywiście takie rzeczy cieszą, ale należy jednak uważać i w pierwszej kolejności przeskanować pamięć.

Nie pożyczamy nikomu swojej szczoteczki do zębów czy ręcznika, żeby uniknąć zakażenia wirusami, bakteriami, grzybami. Tak samo traktujmy swój komputer – to nasza własność, na której mogą znajdować się wrażliwe dane, więc w miarę możliwości ograniczajmy dostęp do niego osobom postronnym.

Drugi sposób, który jest powszechnie wykorzystywany, to rozsyłanie łańcuszków. Na pewno sam dostałeś kiedyś już wiadomość, w której byłeś proszony o przesłanie jej dalej, bo w przeciwnym wypadku los odwróci się od ciebie, nie wygrasz miliona w totka, a twój dentysta dostanie zawału podczas borowania twojego zęba. Niby nie wierzysz, lecz dmuchasz na zimne, prawda? A może zostałeś poproszony o wsparcie jakiejś akcji charytatywnej, bo bez twojego jednego grosza świat się zawali? Przecież taka kwota to dla ciebie nic, ale jeśli do akcji dołączy rzesza ludzi, to uzbiera się suma wystarczająca na opłacenie czyjegoś leczenia itp. Ile razy sprawdziłeś, czy ktoś, kto jest przedstawiany na zdjęciach lub opisywany w mailu, faktycznie istnieje? Jeden, dwa, trzy…? Zero? No właśnie.

Takim sztandarowym przykładem łańcuszka jest zdjęcie poparzonej Oli, które pojawia się w internecie od 2005 r. Faktycznie, dziecko zostało poparzone, a oszuści wykorzystali w sposób nieludzki ten fakt, prezentując zdjęcie w portalach społecznościowych, mailach i prosząc o wsparcie. W rzeczywistości jednak rodzice Oli nigdy nie prosili o pomoc internautów, a co za tym idzie – żadne pieniądze, które w dobrej wierze zostały przelane na podane konto, nigdy do nich

nie trafiły. Na portalach społecznościowych bardzo często, patrząc na to zdjęcie, użytkownicy udostępniają je kolejnym osobom, myśląc, że ktoś płaci za liczbę udostępnień. Otóż nie, tak nie jest. To tylko droga do zdobycia jak największej ilości danych o użytkownikach. Natomiast dziecko już dawno wydobrzało, bardzo dobrze sobie radzi i zgłasza się do krakowskiego szpitala tylko na konsultacje, jednak oszuści w dalszym ciągu wykorzystują zaistniałą sytuację na potęgę.

Oczywiście to nie jedyne dziecko, nie jedyna sytuacja, którą oszuści wykorzystują i podszywając się pod przerażonych rodziców, błagają o pomoc. Jeśli koniecznie chcesz wesprzeć kogoś w potrzebie, dołączyć do jakiejś akcji, przesłać komuś ubranie, to zacznij od ustalenia, czy komunikat jest prawdziwy, czy ktoś chce tylko wykorzystać twoje dobre serce. Obecnie większość instytucji, fundacji, organizacji ma swoje strony internetowe lub profile w serwisach społecznościowych. Możesz wejść na taką stronę i sprawdzić, czy osoby, które masz zamiar wesprzeć, są umieszczone na listach opublikowanych na tych stronach. Możesz też zwyczajnie zadzwonić do szpitala i zapytać, czy osoba, o której napisano, że została poszkodowana, jest wśród pacjentów, ponieważ chcesz jej pomóc.

Wracając jednak do komputera – pamiętaj, że maile stanowiące łańcuszek mają zazwyczaj załączniki, w których może być dosłownie wszystko. Nie klikaj ich bez potrzeby. To często wystarczy, aby twój komputer stał się dla cyberprzestępców niczym otwarta księga.

Makropolecenie, zwane także makrem – zestaw wielu poleceń zapisany w taki sposób, aby jedno kliknięcie powodowało wykonanie tych poleceń w określonej przez jego autora kolejności.

Znajomi zwykli wysyłać ci prezentacje z cudnymi kotami i takimi słodkimi szczeniaczkami, że grzechem byłoby nie zobaczyć? A czy podczas uruchamiania takiego pokazu slajdów nie zauważyłeś przypadkiem, że na ekranie pojawiła się informacja o tym, że w pliku jest makro? Nie zauważyłeś, bo klikałeś OK, OK i jeszcze raz OK, żeby pozamykać kolejne okna z ostrzeżeniami i nie bardzo chciało ci się czytać, co jest w nich napisane. Nie popełniaj więcej tego błędu.

Pliki, w których umieszczono makropolecenia, są bardzo często nośnikiem wirusów lub innego złośliwego oprogramowania. Makra są istotne z punktu widzenia kogoś, kto tworzy plik – ułatwiają np. formatowanie dokumentu.

Nie są natomiast ważne dla odbiorców. Hakerzy jednak bardzo często, wykorzystując niewiedzę użytkowników, dodają makra do plików. Odbiorca myśli, że makro jest potrzebne do właściwego odtworzenia rzeczonej prezentacji, więc zgadza się na jego uruchomienie mimo kolejnych ostrzeżeń wysyłanych przez system operacyjny, a często także mimo prób zablokowania pliku przez program antywirusowy. W efekcie komputer zostaje zainfekowany.

Partycja – logiczny obszar dysku twardego, który może być sformatowany w odpowiednim systemie plików. Uszkodzenie jednej partycji nie wpływa na inną. Jeśli przykładowo na dysku zostały wydzielone trzy obszary, to zazwyczaj pierwszy jest nazywamy dyskiem C i umieszczamy na nim pliki odpowiedzialne za funkcjonowanie systemu operacyjnego. Kolejne partycje to najczęściej D i E (ale nie jest to regułą). Na nich przechowuje się takie pliki, jak zdjęcia lub dokumenty.

Kolejna ważna sprawa to przechowywanie danych. Korzystając z komputera przez wiele lat, wyrabiamy w sobie pewne nawyki segregowania plików, układania ich we właściwych folderach. Kiedy otwierasz szafę i okazuje się, że skarpety leżą w miejscu koszulek, a tam, gdzie powinien być garnitur, wisi sukienka żony, jesteś skonsternowany, a często po prostu zły. Podobnie powinno być z komputerem – zachowasz w nim porządek, jeżeli utworzysz foldery, a w nich będziesz tematycznie zapisywać pliki lub inne foldery. Pamiętaj, aby nie iść na łatwiznę i nie zapisywać prywatnych danych w domyślnych folderach, takich jak **Dokumenty**, **Moje obrazy** itp. Uzyskanie dostępu do tych folderów jest bardzo łatwe. Dlatego warto przez chwilę poczuć się jak informatyk z krwi i kości i podzielić dysk na co najmniej dwie partycje lub dokupić dysk.

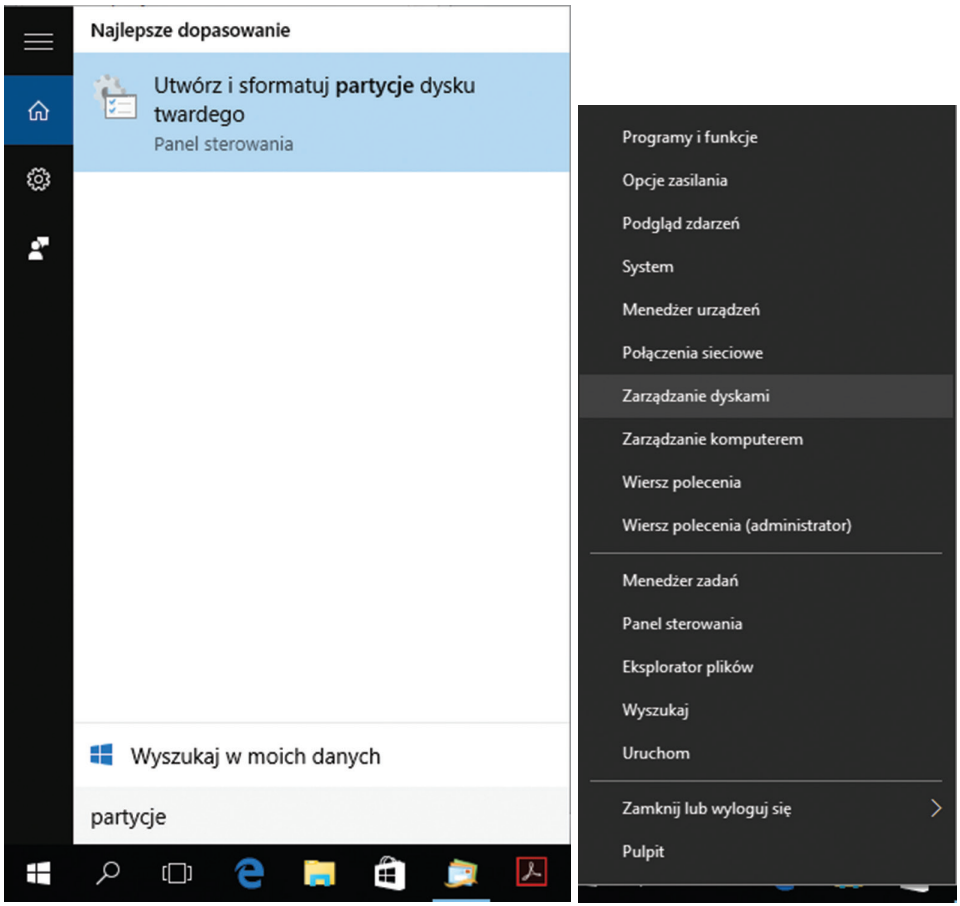
Podziału dysku na partycje dokonuje się zazwyczaj podczas pierwszej instalacji systemu operacyjnego. Dyski są bardzo pojemne, więc śmiało można założyć, że pierwsza partycja, którą przeznacza się na instalację systemu oraz programów użytkowych, powinna mieć co najmniej 200–250 GB. Pozostałą część dysku można podzielić dowolnie.

Jeżeli kupiłeś komputer, na którym jest już zainstalowany system Windows, to może się okazać, że została utworzona tylko jedna partycja. Zanim zaczniesz instalować nowe programy, zapisywać prywatne pliki, również zastanów się nad partycjonowaniem dysku. W internecie jest wiele programów, które mają w tym

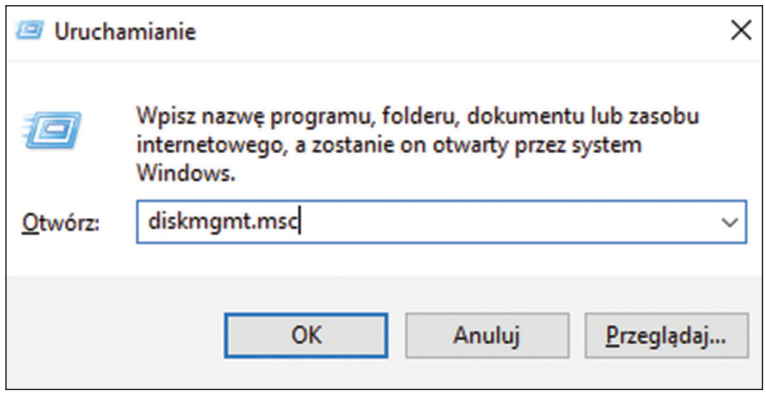
pomóc, jednak nie ma większego sensu ich pobierać. System Windows został wyposażony we własne narzędzia, które umożliwiają podział na partycje.

1. Kliknij na pasku zadań ikonę lupy, a następnie w polu wyszukiwania wpisz „partycje”. Wybierz wynik wyszukiwania albo kliknij przycisk **Start** prawym przyciskiem myszy i z menu kontekstowego wybierz **Zarządzanie dyskami** (rys. 2).

   Możesz też nacisnąć kombinację klawiszy **Windows+R**, a następnie w okienku wpisać diskmgmt.msc i kliknąć **OK** (rys. 3).

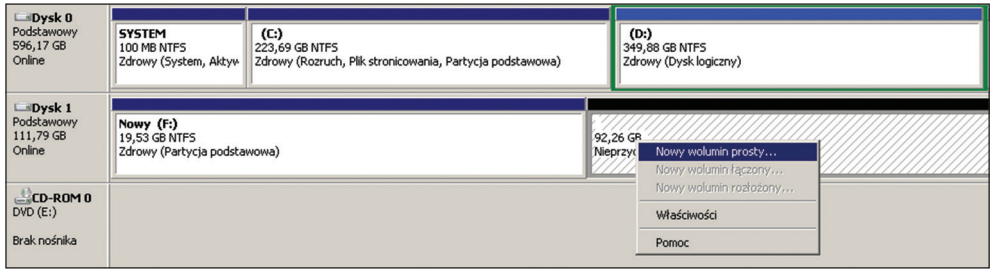


Rysunek 2. Uruchamianie narzędzia do tworzenia partycji na dysku w systemie Windows 10



Rysunek 3. Uruchamianie narzędzia służącego do partycjonowania dysku

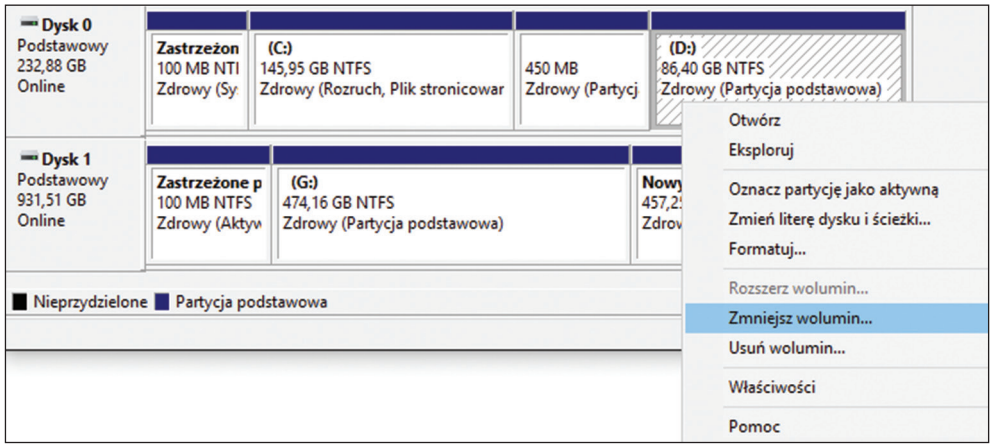
2. W konsoli znajdują się wszystkie informacje o istniejących partycjach oraz nieprzydzielonym jeszcze miejscu. Jeżeli dysk jest nowy, to może się okazać, że nieprzydzielonego miejsca jest naprawdę sporo. Kliknij je wówczas prawym przyciskiem myszy i z menu kontekstowego wybierz **Nowy wolumin prosty** (rys. 4).



Rysunek 4. Tworzenie nowej partycji

3. W kolejnych oknach należy określić rozmiar partycji, literę dysku (zazwyczaj wybiera się C jako partycję systemową, a kolejne litery alfabetu to kolejne partycje), system plików (NTFS), jednostki alokacji (najmniejsza ilość miejsca na dysku, która może być przeznaczona do przechowywania pliku) i wreszcie etykietę woluminu.

4. Jeżeli natomiast całe miejsce na dysku zostało przydzielone do jednej partycji, to najpierw należy ją zmniejszyć, przy czym można ją zmniejszyć wyłącznie o wartość wolnego miejsca znajdującego się na dysku. W tym celu kliknij wybraną partycję prawym przyciskiem myszy i z menu podręcznego wybierz **Zmniejsz wolumin** (rys. 5).



Rysunek 5. Zmniejszanie partycji

5. W kolejnych krokach określ nowy rozmiar partycji.
6. Kiedy uzyskasz nieprzypisane miejsce, możesz ponownie dokonać jego podziału na nowe partycje.

W przypadku komputerów stacjonarnych zamontowanie dodatkowego dysku nie nastręcza żadnych problemów. Sytuacja się komplikuje w przypadku laptopów. W ostatnim czasie jednak na rynku pojawiło się mnóstwo dysków zewnętrznych, które możesz podłączyć sieciowo lub za pomocą kabla, korzystając ze złącza USB (czyli takiego samego, do którego wpinasz pendrive). Obecnie możesz kupić albo dysk twardy (HDD), czyli taki, jaki od lat montuje się w komputerach, albo dysk nowszej generacji SSD (dysk półprzewodnikowy). SSD jest zdecydowanie bardziej wydajny od HDD, jest też, niestety, droższy.

Jeżeli prowadzisz firmę, udzielasz się w klubach czy po prostu masz na dysku pewne ważne informacje, których nie chcesz utracić, to dysk zewnętrzny wydaje się wręcz niezbędny. Te dane, które są naprawdę istotne, powinny mieć swoje

kopie bezpieczeństwa (ang. *backup*). Możesz co prawda zapisywać pliki w chmurze, lecz wówczas należy liczyć się z tym, że łatwo jest je przechwycić. W takiej sytuacji najkorzystniejszym rozwiązaniem wydaje się właśnie dysk zewnętrzny. W razie awarii komputera, uszkodzenia dysku w komputerze, dane na dysku zewnętrznym pozostają nienaruszone.

Jeśli nie możesz akurat pozwolić sobie na zakup dysku, to prześlij kopie istotnych plików do chmury. Najpopularniejszymi rozwiązaniami są: Dysk Google, OneDrive i Dropbox. Wybierz taką opcję, która będzie najlepsza zarówno pod względem pojemności, jak i finansów. Sprawdźmy, jak wygląda sytuacja w przypadku tych trzech usług.

Dysk Google jest usługą bezpłatną. Możesz skorzystać z 15 GB miejsca. Wydaje się, że to dosyć dużo i tak jest, jeżeli na dysku umieszczasz głównie dokumenty tekstowe. Jeżeli przechowujesz na nim zdjęcia i filmy, to ilość miejsca bardzo szybko zaczyna topnieć.

Tyle samo proponuje Microsoft w usłudze **OneDrive**. Tu jednak jest możliwość uzyskania dodatkowej bezpłatnej przestrzeni jako wynagrodzenia za polecenie usługi innym użytkownikom. Oczywiście muszą skorzystać z tej usługi, abyśmy zostali nagrodzeni. Możliwe jest też wykupienie dodatkowej przestrzeni dyskowej – obecnie (początek 2016 r.) miesięczny abonament za 50 GB wynosi 7,99 zł.

Z Dysku Google możesz korzystać, jeżeli tylko masz zarejestrowane konto w usługach Google. OneDrive wymaga rejestracji w usługach Microsoft – zazwyczaj musisz założyć konto podczas wstępnej konfiguracji systemu Windows lub po zakupieniu dowolnego programu Microsoft, np. pakietu biurowego.

Nieco inaczej jest w przypadku **Dropboksa**. Wystarczy, że posiadasz dowolny adres e-mail, aby skorzystać z tej usługi. Tutaj jednak darmowa przestrzeń dyskowa jest o wiele mniejsza – masz do dyspozycji tylko 2 GB. Przekładając to na pliki, można powiedzieć, że wystarczy to na jeden lub dwa pełnometrażowe filmy lub album ze zdjęciami z wakacji. Druga opcja to wykupienie abonamentu miesięcznego – tutaj koszt wynosi 9,99 € miesięcznie, czyli zdecydowanie więcej niż w usłudze OneDrive. Przestrzeń jednak jest nieporównywalna – otrzymujesz za tę kwotę aż 1 TB, czyli dwadzieścia razy więcej miejsca.

Używanie takich dysków w chmurze nie jest niczym skomplikowanym. Po uruchomieniu eksploratora plików pojawiają się odpowiednio foldery o nazwach GoogleDrive (lub Dysk Google), OneDrive lub Dropbox. Kopiujemy do

nich wybrane pliki i dajemy komputerowi czas na ich przesłanie (trwa to odrobinę dłużej niż przy zapisywaniu plików na dysku komputera).

1.5. Nie przesyłaj niezabezpieczonych danych

Każdy z nas musi czasami przekazać pewne informacje innym osobom – mogą to być archiwalne dokumenty, które są podstawą sprawy spadkowej, szczegółowe dane osobowe, informacje o realizowanych projektach, dane techniczne nowego produktu lub loginy i hasła dostępu do firmowego konta bankowego. Takie dane staraj się przekazywać tylko osobiście lub po odpowiednim zabezpieczeniu za pośrednictwem kuriera. Niewskazane jest przesyłanie ich przez internet. Jeżeli sprawa jest bardzo pilna, to postaraj się część danych przesłać jednym kanałem, a część innym, i zadbaj o to, aby były zabezpieczone hasłem.

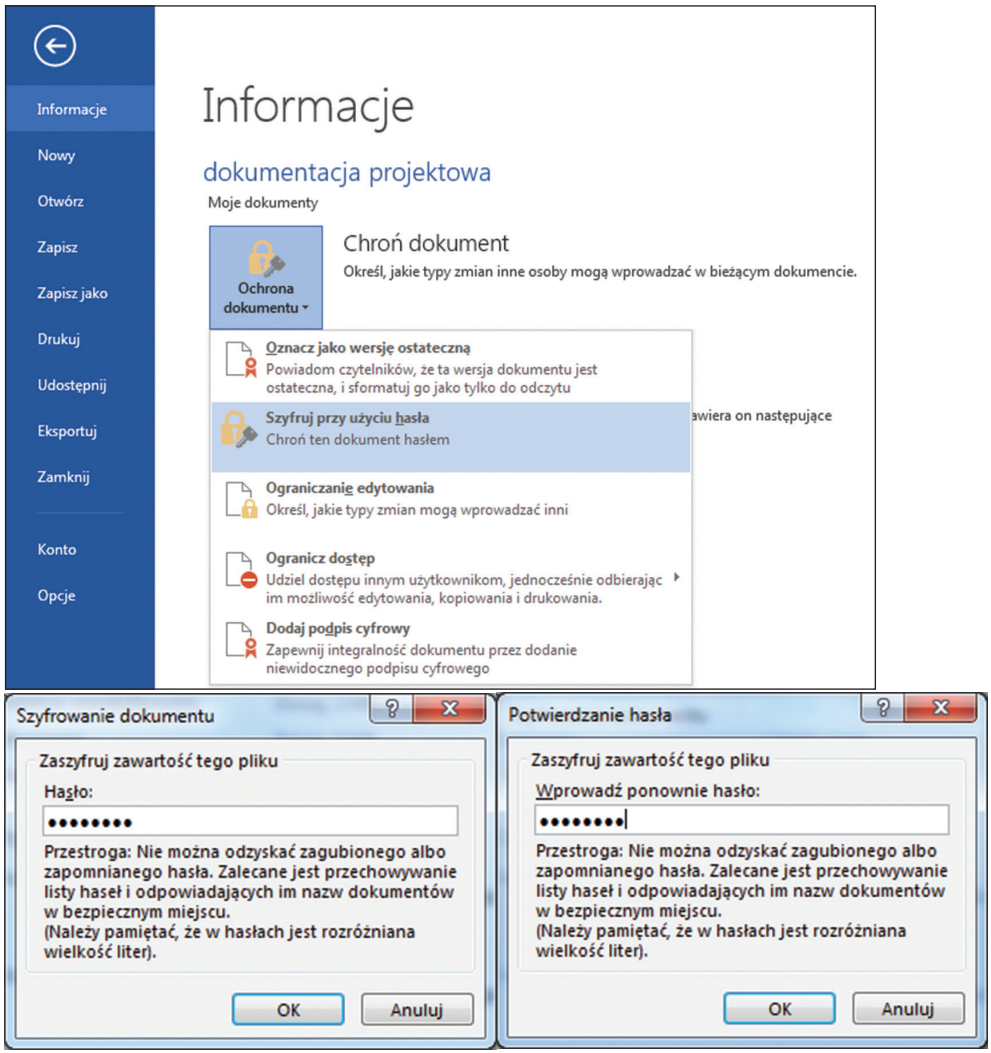
Przesyłając pliki za pomocą poczty elektronicznej lub komunikatorów internetowych, również warto je zabezpieczyć. W przypadku osób prywatnych najczęściej wystarczy zastosowanie podstawowych środków ochrony, jak zabezpieczenie pliku hasłem. Dla cyberprzestępców cenniejsze są oczywiście zasoby firmowe lub rządowe. Natomiast osoby, które przypadkowo wchodzą w posiadanie naszych plików, zazwyczaj nie dysponują na tyle dużą wiedzą, aby łamać zabezpieczenia. Sprawdźmy zatem, jak najszybciej i najłatwiej zadbać o pliki.

1.5.1. Zaszyfruj pliki

Wiele aplikacji pozwala na nadanie plikom haseł, które w nich zapisujemy. Taką opcję znajdziesz między innymi w jednym z najpopularniejszych pakietów biurowych, Microsoft Office. Przypuśćmy, że chcemy chronić dokument tekstowy. W przykładzie pokazany jest Microsoft Word 2013, jednak w innych wersjach tego programu operacja przebiega w ten sam sposób.

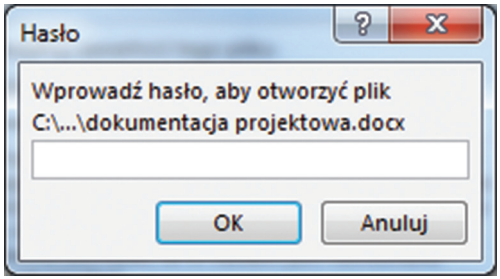
1. Zapisz plik, klikając kartę **Plik**, następnie **Zapisz jako** i nadając mu nazwę.
2. Następnie ponownie kliknij kartę **Plik**.
3. Masz tu dostępną opcję **Chroń dokument**. Jej wybranie spowoduje rozwinięcie listy, na której możesz zaznaczyć, w jaki sposób dokument ma być chroniony. Wybierz **Szyfruj przy użyciu hasła**.

4. Zostaje wyświetlone okno, w którym należy wprowadzić hasło.
5. Po kliknięciu **OK** pojawia się następne okno, w którym powtórnie wprowadź to samo hasło i jeszcze raz kliknij **OK** (rys. 6).



Rysunek 6. Zabezpieczanie dokumentu tekstowego hasłem

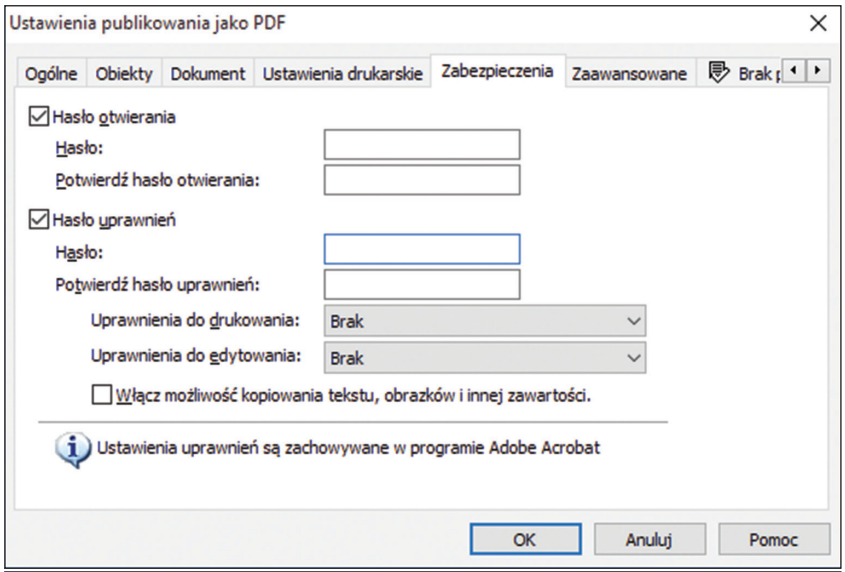
Jeżeli zamkniesz plik, a następnie spróbujesz go powtórnie otworzyć, to zostanie wyświetlone okienko, w którym należy wpisać ustawione wcześniej hasło (rys. 7). W przeciwnym przypadku plik nie zostanie otwarty.

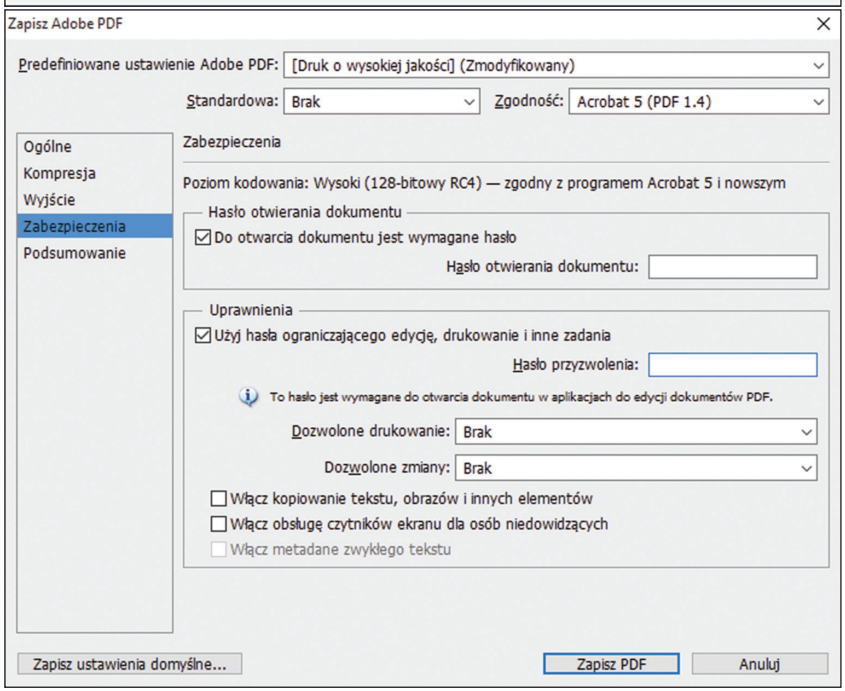


Rysunek 7. Otwieranie dokumentu tekstowego zabezpieczonego hasłem

Dokładnie te same opcje znajdziesz w pozostałych programach pakietu. Zauważ, że poniżej widnieje opcja **Ograniczenie edytowania**. Umożliwia ona ustawienie hasła, bez podania którego użytkownik nie będzie mógł wprowadzać zmian do pliku. Takie jednak hasło nie zabezpiecza przed przejrzeniem zawartości – każdy, kto ma dostęp do pliku, może go odczytać.

Jeśli zajmujesz się grafiką komputerową, składem publikacji przeznaczonych do druku lub zamieszczasz je na stronach internetowych, to często generujesz pliki w formacie PDF. Także i one mogą być chronione hasłem. Po co? Choćby po to, że nieraz zawierają np. projekty techniczne przeznaczone tylko dla określonych osób lub zawartość plików udostępniasz osobom, które wniosły opłatę, kupiły książkę i otrzymały z nią kod dostępu do pliku. Hasło można wprowadzić w ustawieniach publikowania pliku jako PDF, najczęściej w zakładce **Zabezpieczenia**. Tu, jak w przypadku oprogramowania biurowego, również masz możliwość wprowadzenia hasła chroniącego plik zarówno przed otwarciem, jak i przed edycją (rys. 8). Pliki PDF mogą być zabezpieczane hasłem w wersjach PRO, takich aplikacji jak Adobe Reader czy Adobe Acrobat. W podstawowych wersjach takich opcji nie znajdziemy. Konieczne jest zakupienie pełnej wersji lub wykupienie abonamentu.





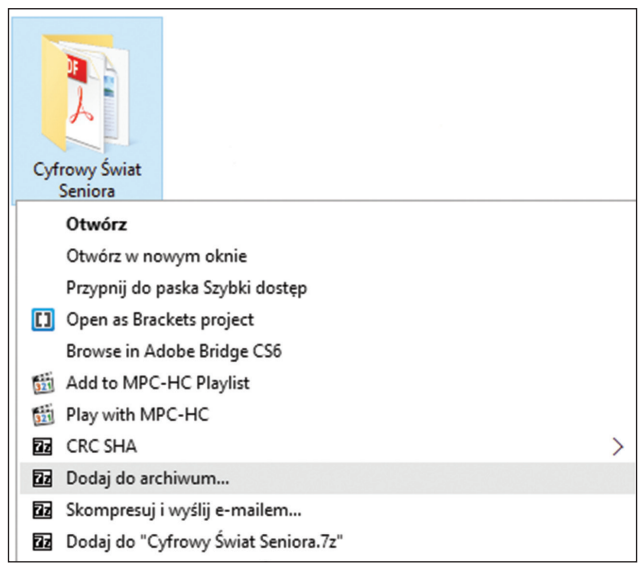
Rysunek 8. Zabezpieczanie plików PDF hasłem w programach Corel i Photoshop

1.5.2. Spakuj pliki

Bardzo często hasłami są zabezpieczane pliki **archiwum**, nazywane też **plikami skompresowanymi** lub **spakowanymi**. Ich zawartość stanowią zwykle inne pliki lub foldery, które na skutek kompresji (pakowania) są umieszczane w jednym pliku mającym mniejszy rozmiar. Z pakowaniem plików jest podobnie jak z pakowaniem walizki – wydaje się, że do środka już nic się nie zmieści, ale odpowiednio przyłożona siła sprawia, że udaje nam się jeszcze upchnąć dodatkową bluzkę, niezbędną książkę i szpilki, bez których wieczór byłby stracony. Dzięki spakowaniu plików lub folderów ich przesłanie przez internet jest łatwiejsze – nie musisz załączać każdego pliku osobno, lecz wystarczy, że wyślesz jeden zbiorczy plik.

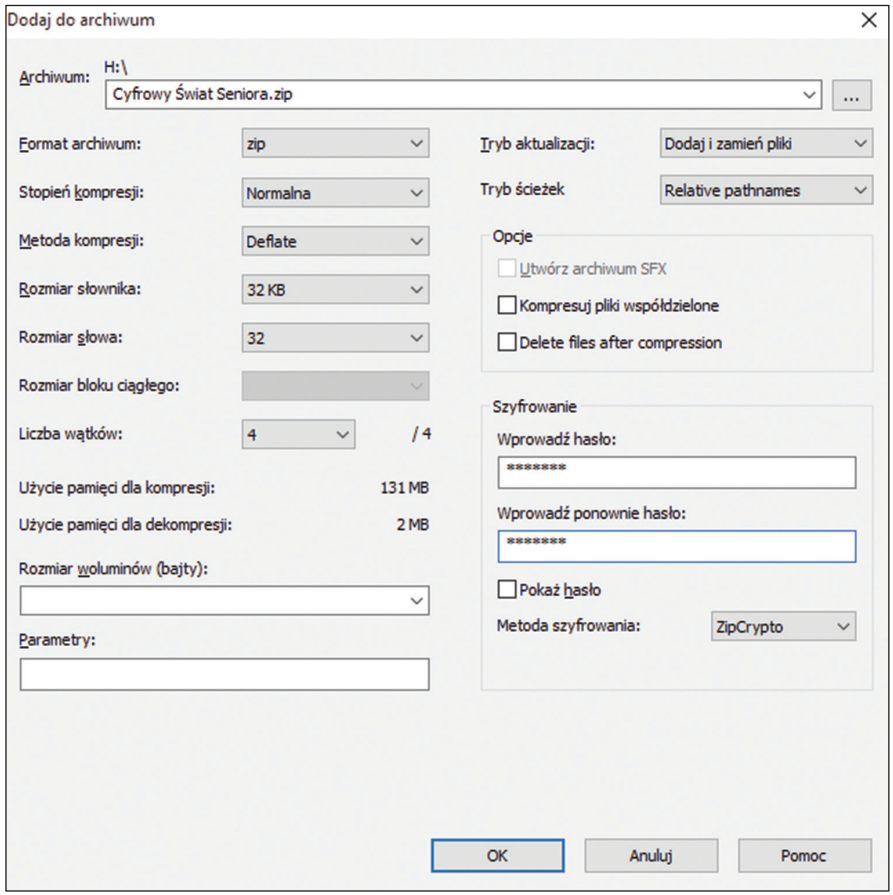
Najbardziej rozpowszechnione formaty plików skompresowanych to .zip i .rar. Natomiast jednym z najpopularniejszych programów jest Easy 7-Zip, który możesz pobrać bezpłatnie z internetu. Podstawowe polecenia tego programu są umieszczane w menu podręcznym.

1. Jeśli chcesz spakować wybrane pliki lub foldery, to zaznacz je w eksploratorze plików i kliknij zaznaczenie prawym przyciskiem myszy.
2. Z menu kontekstowego wybierz **Dodaj do archiwum** (rys. 9).



Rysunek 9. Archiwizowanie pliku

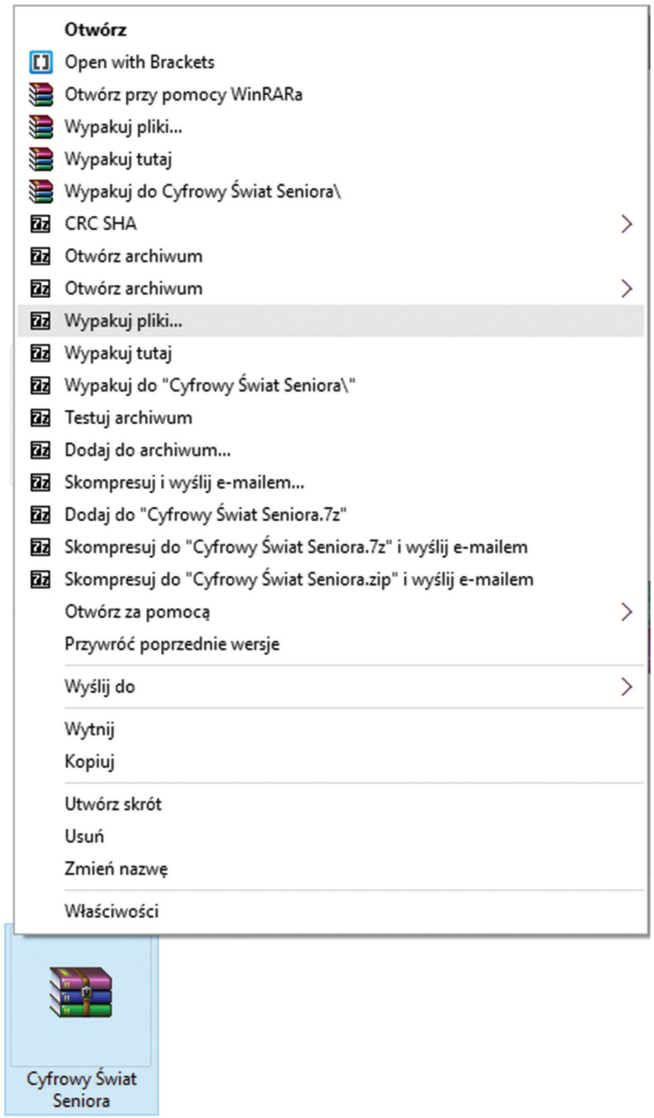
3. W oknie dialogowym, które pojawi się na ekranie, zaznacz opcje kompresji: ustal nazwę pliku docelowego i, jeśli plik ma być chroniony hasłem, w obszarze **Szyfrowanie** wprowadź hasło, po czym je potwierdź, wprowadzając je ponownie w kolejnym polu. Następnie kliknij **OK** (rys. 10).



Rysunek 10. Zabezpieczanie hasłem pliku skompresowanego

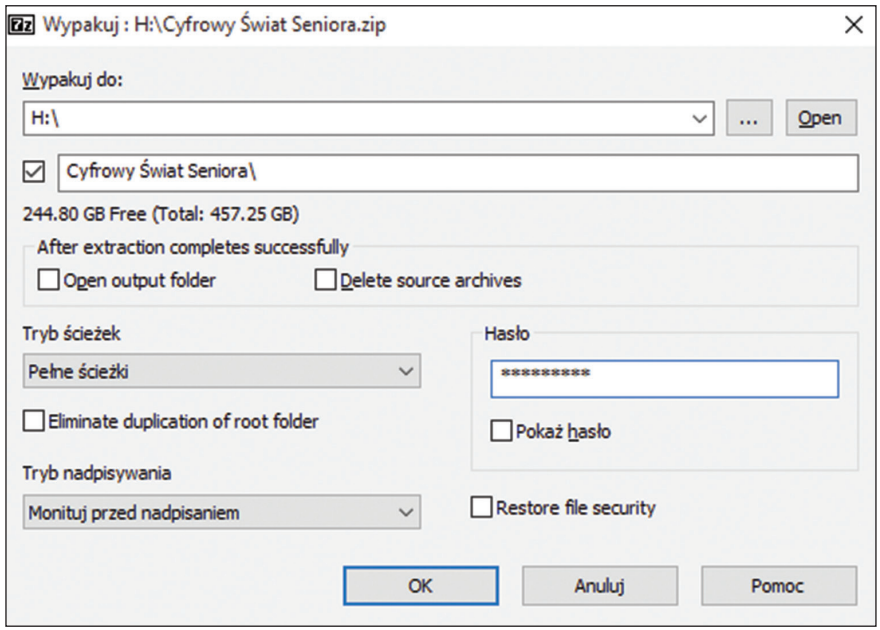
Spróbuj teraz wypakować skompresowany plik.

1. W eksploratorze plików prawym przyciskiem myszy kliknij wybrany plik.
2. Z menu kontekstowego wybierz polecenie **Wypakuj pliki** (rys. 11).



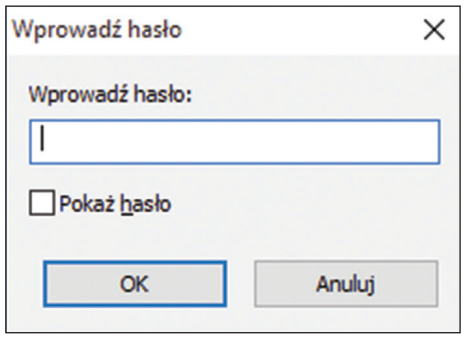
Rysunek 11. Dekompresja pliku

3. Zostaje wyświetlone okno, w którym powinieneś ustalić docelową lokalizację plików oraz wpisać ustalone wcześniej hasło (rys. 12).



Rysunek 12. Wprowadzenie hasła wymaganego do wypakowania pliku

4. Jeśli nie wprowadzisz hasła, lecz klikniesz **OK**, to pojawi się kolejne okno dialogowe, w którym zostaniesz poproszony o właściwe hasło. W przypadku braku hasła pliki nie zostaną wypakowane, nie zobaczysz więc ich zawartości (rys. 13).

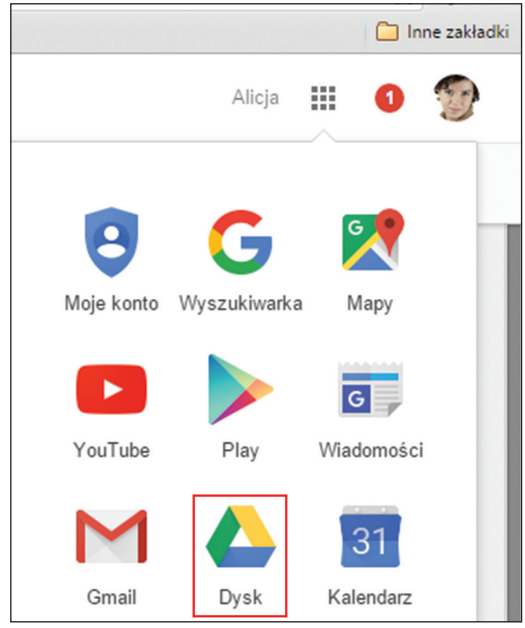


Rysunek 13. Podawanie hasła w celu wypakowania plików

1.5.3. Korzystaj z chmury

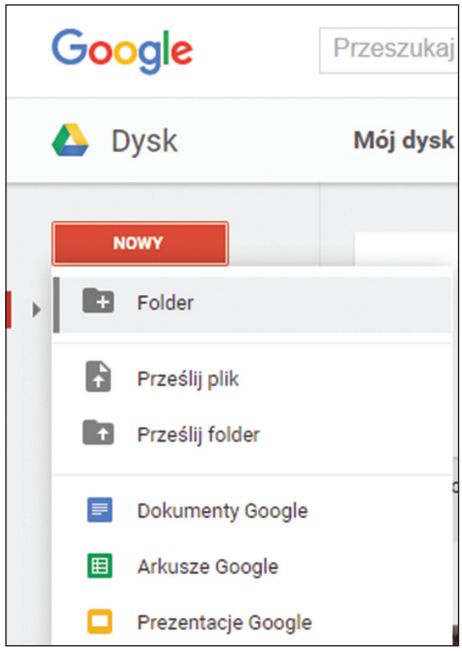
Bezpieczniejszym sposobem (co nie oznacza jednak, że plików nie da się przechwycić) wydaje się umieszczanie danych w chmurze i udostępnianie ich wybranym użytkownikom. Należy przy tym uważać, aby nie stosować zawsze udostępniania domyślnego, ponieważ może się okazać, że jest to udostępnianie publiczne. Sprawdźmy, jak wygląda takie dzielenie się plikami w najpopularniejszych obecnie usługach, czyli Dysku Google, OneDrivie oraz Dropboksie. Wszystkie te usługi działają w wersji webowej, desktopowej oraz mobilnej. W związku z tym, że nie każdy użytkownik instaluje na swoim urządzeniu aplikacje odpowiadające wybranym usługom, przetestujemy wersje webowe, które wymagają tylko zalogowania się. Na początek utwórz dowolny plik, który będziesz kopiował do folderu w wybranej usłudze – nie ma znaczenia, w jakim formacie. Może to być zarówno obraz, jak i zwykły plik tekstowy.

1. Jeżeli masz zarejestrowane konto w usługach Google, to otwórz przeglądarkę internetową i w pasku adresu wpisz `drive.google.com`, po czym się zaloguj. Możesz też zalogować się do dowolnej usługi Google, następnie kliknąć w prawym górnym rogu okna przycisk i z menu wybrać **Dysk** (rys. 14).



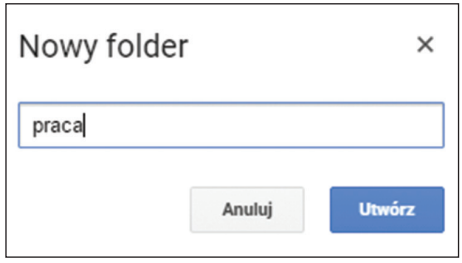
Rysunek 14. Uruchamianie usługi Dysk Google

2. Tak samo jak na dysku komputera, tak i tutaj powinieneś mieć wszystko uporządkowane za pomocą folderów. 15 GB to jednak sporo miejsca i jeżeli pliki będziesz umieszczał w głównym folderze, to niedługo się w nich pogubisz. Załóżmy, że pierwszy folder będzie nosił nazwę „praca". W lewej części okna jest menu – kliknij **Nowy**, a następnie wśród rozwiniętych opcji wybierz **Folder** (rys. 15).



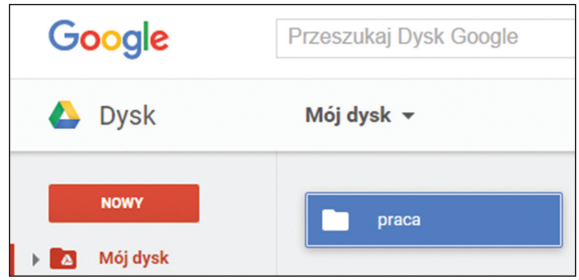
Rysunek 15. Tworzenie nowego folderu w usłudze Dysk Google

3. Zostaje wyświetlone okno, w którym wpisz nazwę folderu i ją zaakceptuj, klikając **Utwórz** (rys. 16).



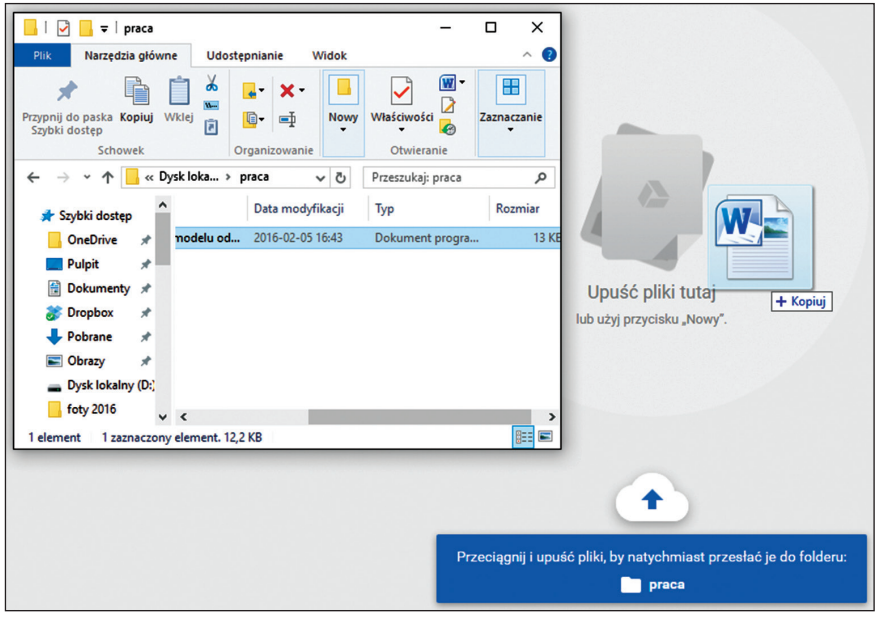
Rysunek 16. Nadawanie nazwy folderowi

4. Folder jest już gotowy. Aby do niego wejść, dwukrotnie kliknij jego nazwę (rys. 17).



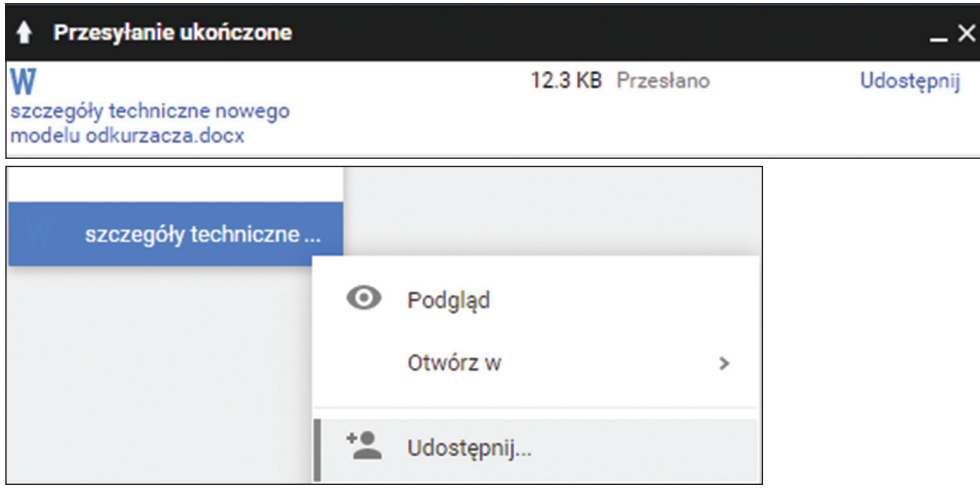
Rysunek 17. Nowy folder

5. Teraz swój plik umieść w folderze „praca". Uruchom eksplorator plików, za pomocą kliknięć znajdź plik przeznaczony do skopiowania i wskaż go kursorem. Jednocześnie wciśnij lewy przycisk myszy i przytrzymując go, przeciągnij plik do folderu. Kiedy obok ikony pliku zobaczysz dymek z treścią + **Kopiuj**, zwolnij przycisk myszy (rys. 18).



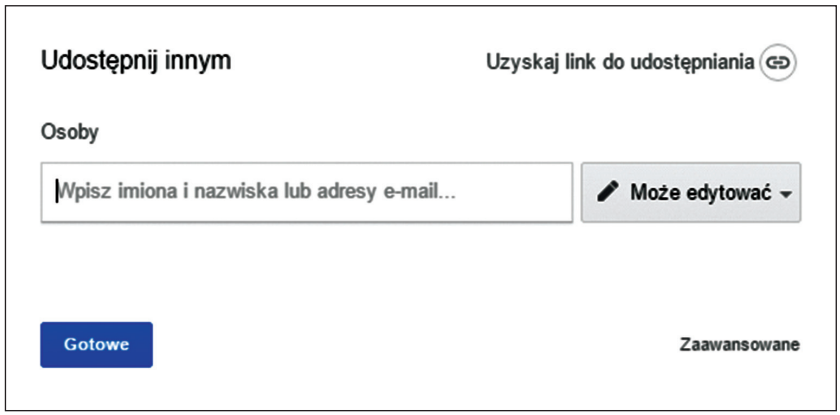
Rysunek 18. Kopiowanie pliku na Dysk Google

6. W prawym dolnym rogu okna jest widoczny status przesyłania pliku. Po zakończeniu tej operacji pojawia się przycisk **Udostępnij**. Jeśli od razu chcesz plik przekazać innemu użytkownikowi, to kliknij ten przycisk. Jeżeli plik będziesz udostępniał później, to możesz zamknąć okno i w dowolnym czasie kliknąć nazwę pliku prawym przyciskiem myszy, a następnie z menu kontekstowego wybrać **Udostępnij** (rys. 19).



Rysunek 19. Opcje udostępniania pliku

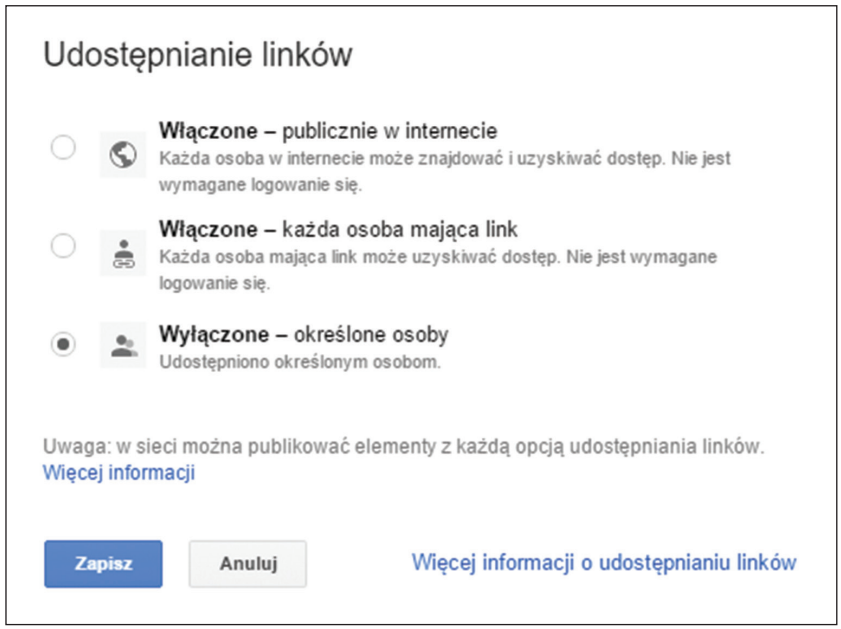
7. W kolejnym oknie możesz wprowadzić adres mailowy osoby, której chcesz udostępnić plik. I teraz mała pułapka – wydaje się, że wszystko jest ustawione prawidłowo, można wysyłać, plik jest bezpieczny. Otóż nie, jeszcze nie jest. Jeżeli plik udostępnisz w takiej formie, każda osoba, która otrzyma od adresata link do twojego pliku, będzie mogła go bez problemu zobaczyć. Kliknij **Zaawansowane** (rys. 20).
8. W obszarze **Kto ma dostęp** na razie jest widoczna informacja, że tylko właściciel może wyświetlać i edytować plik. Kliknij **Zmień** (rys. 21).



Rysunek 20. Udostępnianie pliku za pomocą Dysku Google

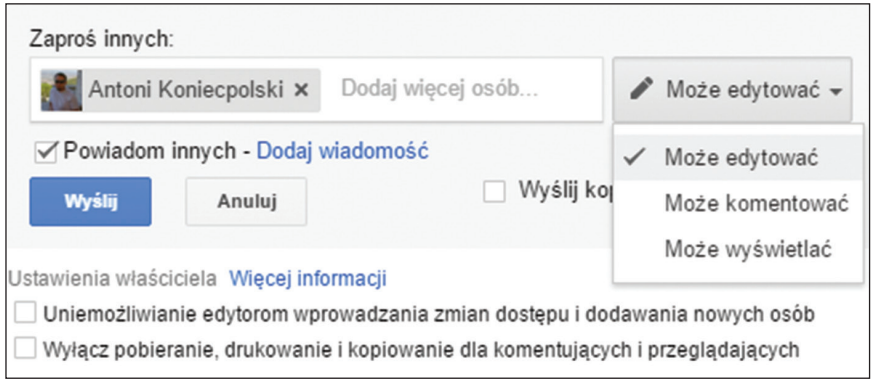
Rysunek 21. Zaawansowane ustawienia udostępniania pliku

9. Masz do dyspozycji trzy opcje udostępniania linków. Aby jak najbardziej zabezpieczyć plik, wybierz **Wyłączone – określone osoby**. Zatwierdź te ustawienia przyciskiem **Zapisz** (rys. 22).



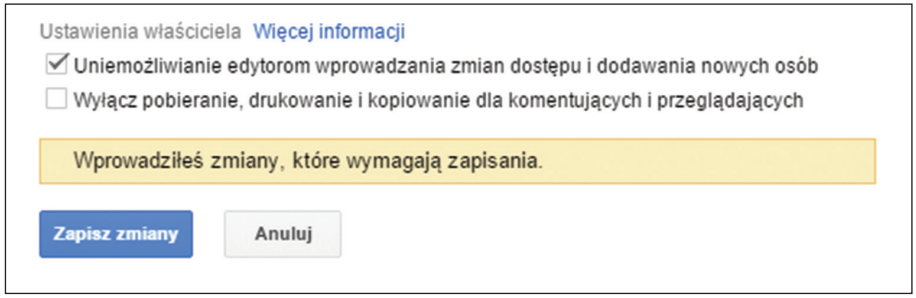
Rysunek 22. Wyłączanie udostępniania publicznego

10. Wreszcie w obszarze **Zaproś innych** wprowadź adres lub adresy e-mail i wybierz z listy, czy odbiorcy będą mogli edytować, komentować, czy tylko wyświetlać plik (rys. 23).



Rysunek 23. Wprowadzanie adresatów i nadawanie im uprawnień

11. Możesz jeszcze wyłączyć możliwość dodawania kolejnych odbiorców przez adresata – po zaznaczeniu tej opcji kliknij **Zapisz zmiany** (rys. 24).



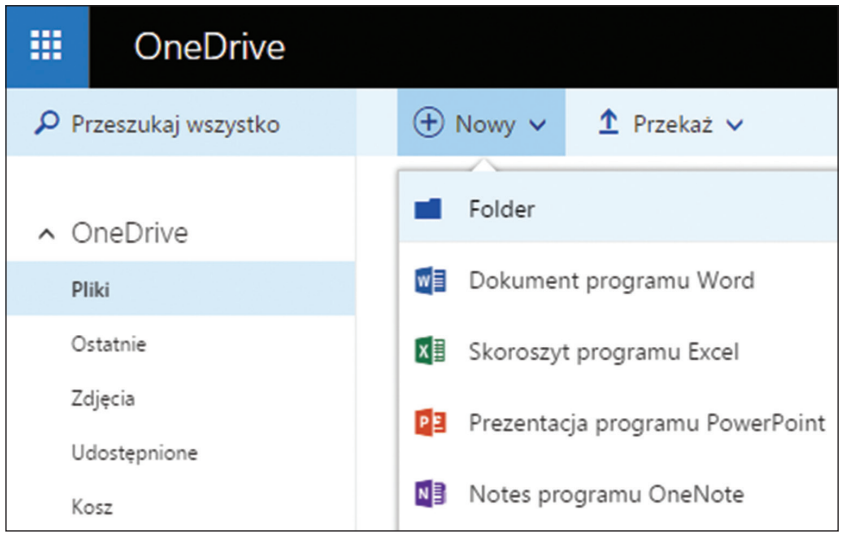
Rysunek 24. Ograniczanie możliwości dalszego udostępniania pliku

12. Po zakończeniu ustawień kliknij **Wyślij**. Następnie przycisk ten zostanie zastąpiony przyciskiem **Gotowe** – kliknij go, aby zamknąć okno.

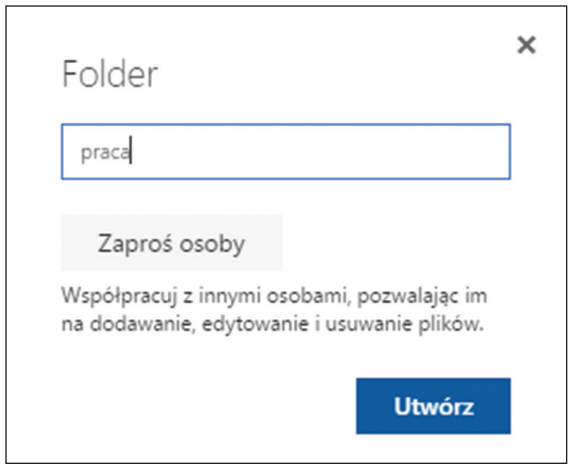
Tak udostępniony plik jest w miarę bezpieczny. Jeżeli nawet ktoś zdobędzie link do pliku, to po jego wpisaniu do przeglądarki pojawi się prośba o zalogowanie. Zalogowanie na inne konto niż konto właściciela pliku lub osób z listy nic kompletnie nie da – pliku nie da się nawet wyświetlić.

Zobaczmy, czy w usłudze OneDrive tak samo możemy zabezpieczyć plik, aby dostęp do niego miały tylko wybrane osoby.

1. Jeżeli jesteś zarejestrowany w usługach Microsoftu, to uruchom przeglądarkę i w pasku adresu wpisz `onedrive.live.com`, a następnie zaloguj się na swoje konto.
2. Kliknij **Nowy** i w menu wybierz **Folder** (rys. 25).
3. W wyświetlonym oknie wpisz nazwę nowego folderu – może być taki sam, jak wcześniej. Następnie kliknij **Utwórz** (rys. 26).

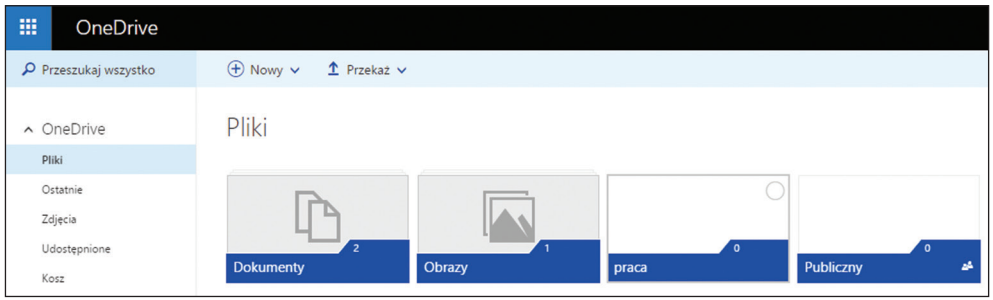


Rysunek 25. Tworzenie nowego folderu w usłudze OneDrive



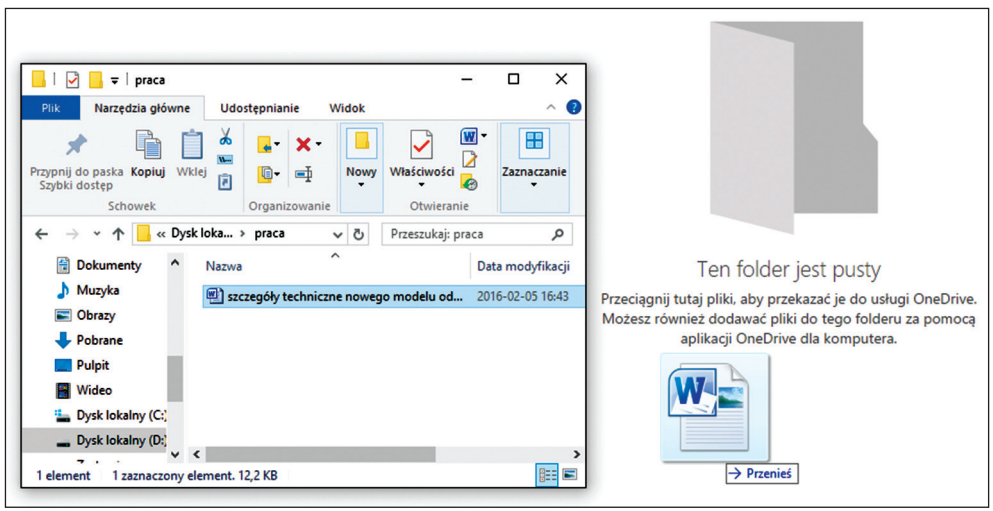
Rysunek 26. Nadawanie nazwy folderowi

4. Folder jest założony – aby go otworzyć, wystarczy kliknąć jego nazwę (rys. 27).



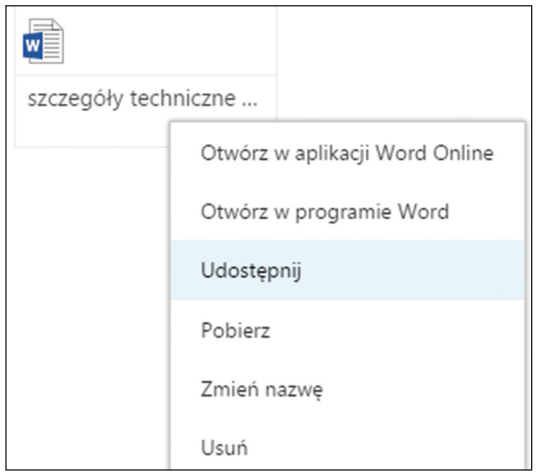
Rysunek 27. Widok folderów w usłudze OneDrive

5. Otwórz eksplorator plików, najedź kursorem na plik, który chcesz skopiować, wciśnij lewy przycisk myszy i przytrzymując go, przeciągnij plik do folderu „praca”. Kiedy pojawi się napis → **Przenieś**, zwolnij przycisk (rys. 28).



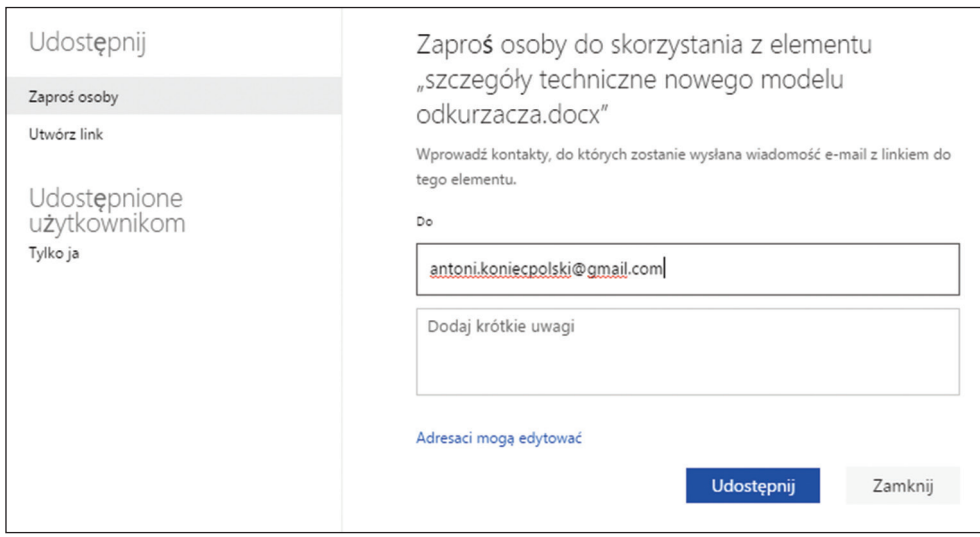
Rysunek 28. Kopiowanie pliku na dysk OneDrive

6. Kliknij przesłany plik prawym przyciskiem myszy i z menu kontekstowego wybierz **Udostępnij** (rys. 29). Możesz też kliknąć przycisk **Udostępnij** umieszczony nad plikiem.



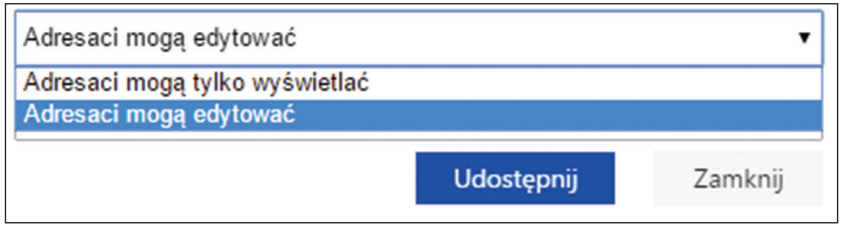
Rysunek 29. Włączanie udostępniania pliku

7. W kolejnym kroku wprowadź adres lub adresy mailowe (rys. 30).



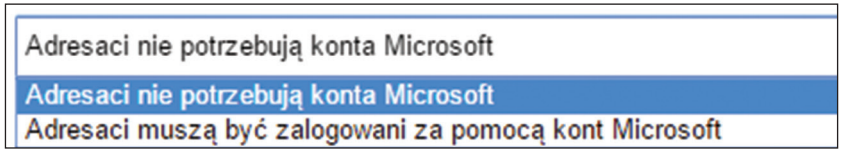
Rysunek 30. Wprowadzanie adresatów

8. Ustal uprawnienia adresatów – tym razem masz do dyspozycji tylko dwie opcje: wyświetlanie oraz edycję (rys. 31).



Rysunek 31. Ustalanie uprawnień adresatów

9. Dodatkowo możesz określić, czy adresaci muszą być zarejestrowani w usługach Microsoftu, czy nie (rys. 32). Pamiętaj jednak, że twoi znajomi korzystają zazwyczaj po prostu z konta mailowego, a jeżeli nawet są zarejestrowani w Microsofcie, to zdarza się, że nie pamiętają, jakiego adresu podczas tej rejestracji używali lub jakie wprowadzili hasło. Ważne jest również to, że nawet jeśli wyświetlenie lub edycja pliku wymagają posiadania konta w usługach Microsoftu, to nie stanowi to zbyt dużego zabezpieczenia dla pliku – każda osoba, która zaloguje się do tych usług, może udostępniać plik kolejnym osobom.

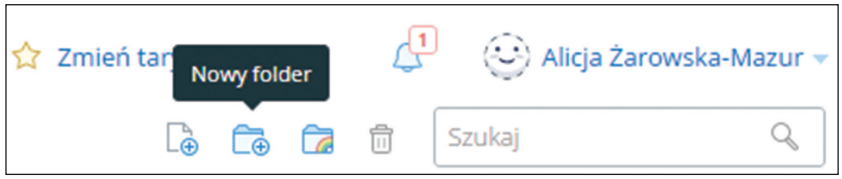


Rysunek 32. Określanie sposobu udostępniania pliku

Plik jest udostępniony. W przeciwieństwie jednak do Dysku Google, każda osoba, która otrzyma link, ma dostęp do pliku. Nie ma tu również opcji ograniczania dalszego udostępniania. Oczywiście ten sposób przekazywania informacji i tak jest bezpieczniejszy niż za pomocą poczty elektronicznej lub komunikatora, lecz, niestety, na razie pozostawia sporo do życzenia.

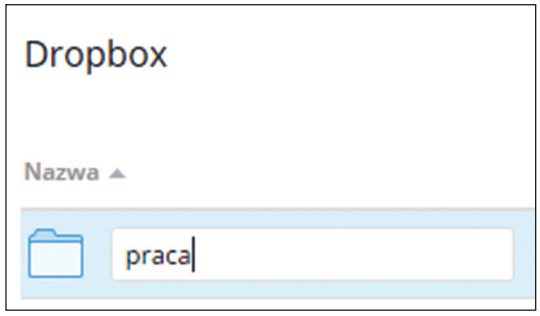
Pozostaje nam ostatnia usługa. Nie wymaga ona zakładania konta ani w usługach Google, ani Microsoftu. Możesz korzystać z dowolnego adresu e-mail, który masz.

1. Uruchom przeglądarkę i w pasku adresu wpisz `dropbox.com`.
2. Jeżeli jesteś już zarejestrowany, to zaloguj się. Jeśli nie, to skorzystaj z opcji **Utwórz konto**.
3. Utwórz nowy folder, klikając przycisk (rys. 33).



Rysunek 33. Tworzenie nowego folderu w usłudze Dropboksa

4. Nadaj folderowi nazwę i zatwierdź ją klawiszem **Enter** (rys. 34).

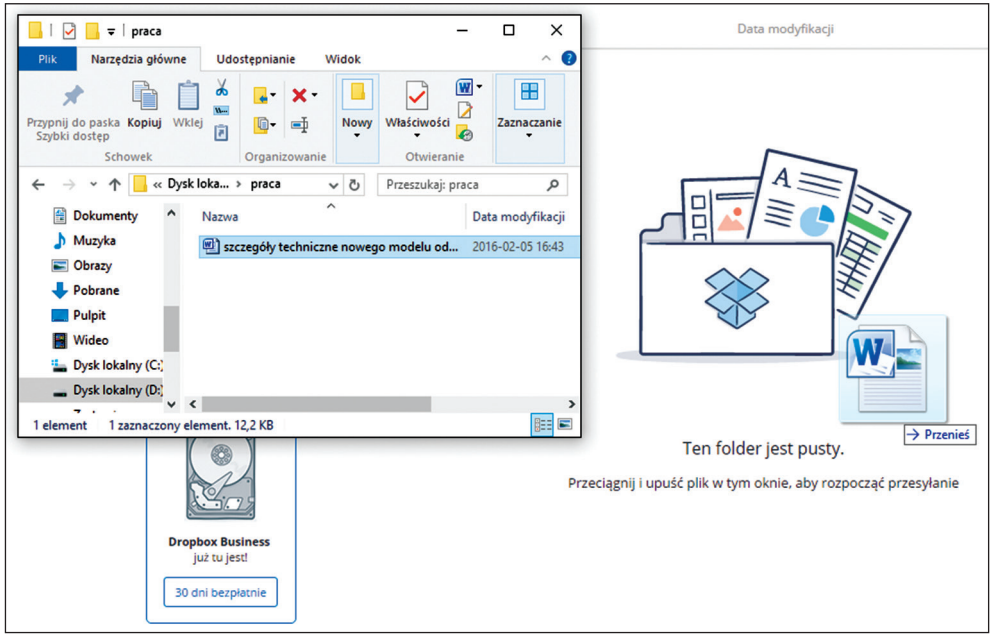


Rysunek 34. Nadawanie nazwy folderowi

5. Najedź kursorem na nazwę i ją kliknij, aby otworzyć folder (rys. 35).

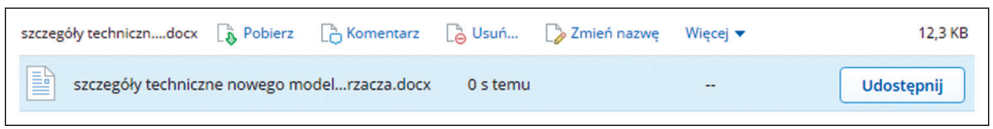
Rysunek 35. Widok nowego folderu

6. Na razie folder jest pusty. Podobnie jak w pozostałych usługach, uruchom eksplorator plików i przeciągnij plik do folderu (rys. 36).



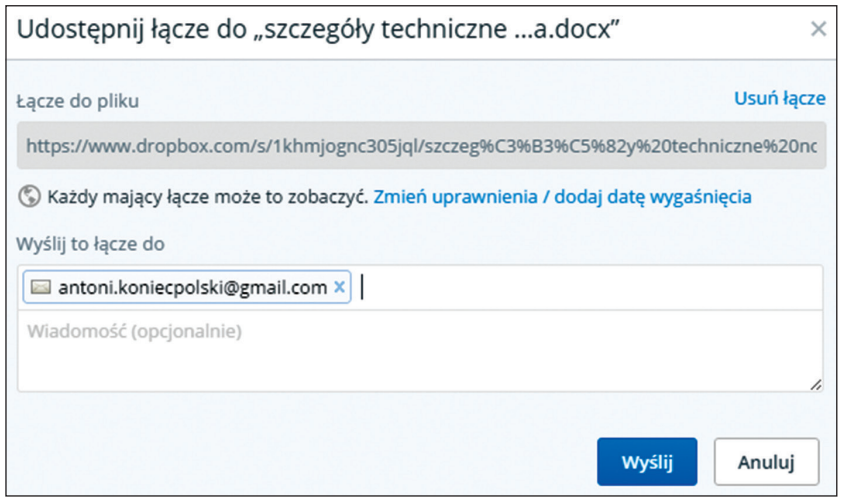
Rysunek 36. Kopiowanie pliku do folderu na Dropboksie

7. Po przesłaniu pliku obok jego nazwy pojawi się przycisk **Udostępnij**. Kliknij go (rys. 37).



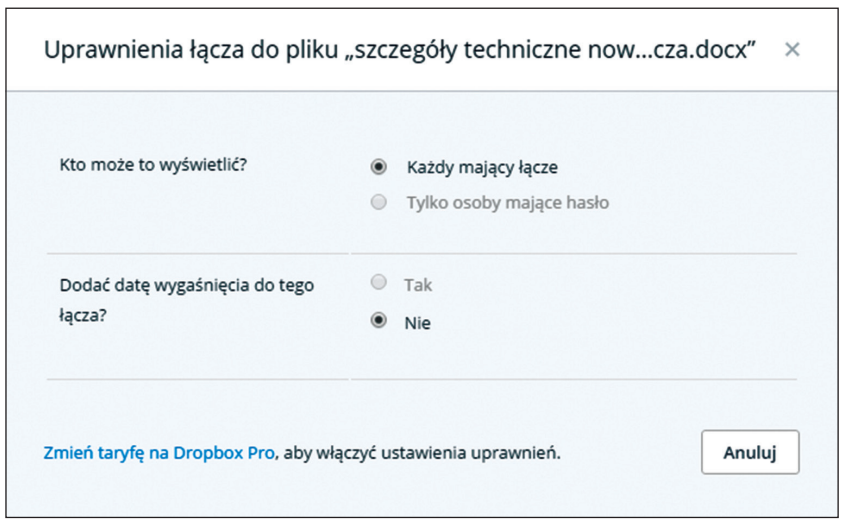
Rysunek 37. Udostępnianie pliku

8. W podstawowej wersji usługi możesz wprowadzić adresatów, a następnie kliknąć **Wyślij** (rys. 38). To oznacza, że każda osoba, która otrzyma link do pliku, może ten plik pobrać lub wyświetlić.



Rysunek 38. Wprowadzanie adresatów

9. Po wykupieniu wyższej taryfy możesz wybrać zmianę uprawnień i zezwolić na wyświetlanie pliku tylko przez osoby dysponujące właściwym hasłem, a także określić, jak długo plik ma być udostępniany (rys. 39).



Rysunek 39. Opcje udostępniania pliku na Dropboksie

Jak widzisz, Dropbox może być bezpieczny, jednak wymaga to wniesienia opłaty abonamentowej. Podsumowując te trzy usługi, okazuje się, że w bezpłatnej, podstawowej wersji największe możliwości daje Dysk Google. Natomiast obsługa wszystkich trzech dysków polega na wykonywaniu bardzo zbliżonych operacji. Na rynku jest mnóstwo innych usług tego typu – zazwyczaj jednak są płatne. Chcąc udostępniać pliki innym użytkownikom, zwykle korzystam z Dysku Google, jeśli natomiast pilnie chcę wykonać kopię bezpieczeństwa, to wybieram OneDrive lub Dropbox. Każda z tych usług ma wady i zalety. Nie można jednak ślepo ufać żadnej z nich – zalecany jest zdrowy rozsądek. Pamiętaj, że w dalszym ciągu to tylko sprzęt i oprogramowanie – jeżeli wszystko działa, to świetnie, ale zawsze należy liczyć się z tym, że takie usługi mogą paść np. ofiarą hackingu. Jeśli to tylko możliwe, ograniczaj liczbę użytkowników mających dostęp do plików, wyłączaj opcję dalszego udostępniania i pamiętaj, aby ustalić termin wygaśnięcia dostępu lub zapisuj w kalendarzu, kiedy taki dostęp chcesz wyłączyć.