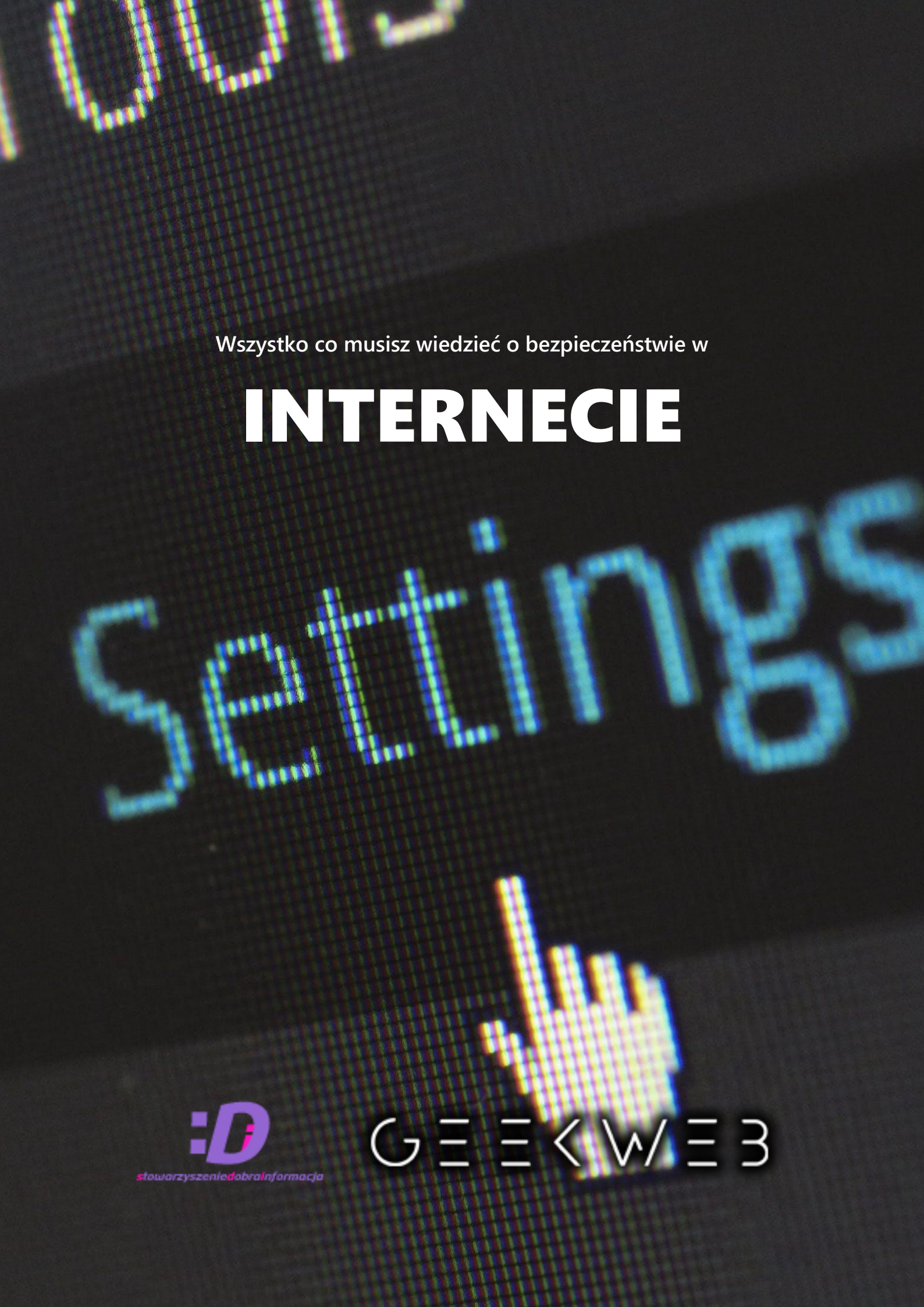


Wszystko co musisz wiedzieć o bezpieczeństwie w

INTERNECIE

stowarzyszeniedobraInformacja

GEEKWEB

SPIS TREŚCI

Wstęp

W 2020 roku, według raportu Głównego Urzędu Statystycznego, dostęp do Internetu w Polsce miało 90,4 procenta gospodarstw domowych i było to o 3,7 procenta więcej, niż w roku poprzednim. Także w ubiegłym roku odsetek osób w wieku od 16 do 74 roku życia, które kupowały w Internecie towary lub usługi w ciągu ostatnich dwunastu miesięcy wyniósł 60,9 procenta, co było z kolei wzrostem rok do roku o 7 procent. Co czwarty z respondentów GUSu korzystał z możliwości pracy zdalnej. Ponad 98 procent osób w wieku 16–74 w 2020 roku śledziło informacje dotyczące Covid-19. Cały ubiegły rok toczył się zresztą w sieci pod hasłem koronawirus. Znalazło się ono na pierwszym miejscu zarówno polskiego, jak i globalnego zestawienia *Rok w wyszukiwarce Google*. W czwartym kwartale 2019 roku liczba rachunków klientów indywidualnych posiadających umowy umożliwiające dostęp do usług bankowości internetowej w Polsce wyniosła ponad 37 milionów. Aktywnie, czyli logując się przynajmniej raz w miesiącu, z rachunków tych korzysta ponad 18 milionów Polaków. Wszystkie te dane wskazują jednoznacznie, że w Internecie już nie tylko bywamy. W Internecie obecnie żyjemy.

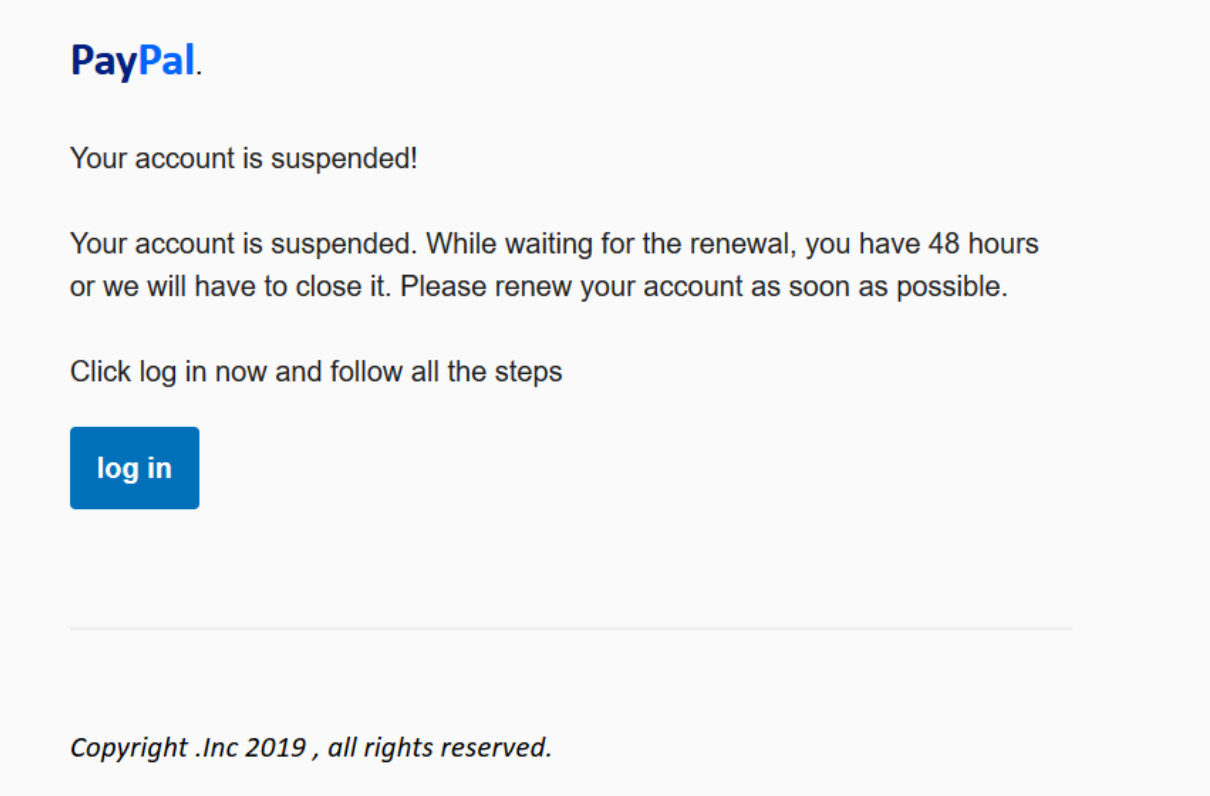
Niestety, wraz z rozwojem kolejnych internetowych narzędzi rośnie również zagrożenie bezpośrednio z tego faktu wynikające. Cyberprzestępczość. Z najnowszej edycji raportu Europolu wynika, że pandemia jeszcze wzmocniła wszystkie znane wcześniej problemy na tym polu. Kluczowe wnioski płynące z tego dokumentu to fakt pozostawania

inżynierii społecznej, czy też socjotechnik, w roli lidera zagrożeń i niejako punktu wyjścia do przeprowadzania kolejnych ataków. Raport IOCTA wskazuje również złośliwe oprogramowanie typu ransomware, jako jedno z najistotniejszych zagrożeń dla użytkowników indywidualnych, ale przede wszystkim organizacji w łańcuchu dostaw, a także ogromne zagrożenie dla infrastruktury krytycznej. Nie można w tym wszystkim zapominać również o dzieciach, których co prawda dotyczyć może nieco inne spektrum zagrożeń, jednak ich charakter jest niemniej niebezpieczny. Czas pandemii pokazał również z jak wielką skalą dezinformacji i ilością informacji całkowicie fałszywych możemy mieć w Internecie do czynienia. Umiejętność filtrowania i docierania do rzetelnych źródeł informacji są dziś niezwykle pożądane i powinny być w arsenale umiejętności każdego użytkownika sieci. Zagrożenia związane z dezinformacją i tzw. fake newsami są bowiem nie tylko powodem *tiktokizacji* debaty publicznej, ale mogą stanowić realne zagrożenie dla ładu i porządku publicznego, a w sytuacjach skrajnych nawet dla bezpieczeństwa narodowego.

Do całej tej układanki dołożyć należy zagrożenia na które podatności nie mamy niemal żadnego wpływu, to np. wycieki danych. Bezpieczeństwo powierzonych jakiemuś dostawcy usług danych leży w jego gestii, ale jako użytkownicy możemy podejść do nich w sposób znacznie roztropniejszy. I to wszystko chcielibyśmy Państwu za pomocą tego poradnika przekazać. Zawarta w nim treść to, mamy nadzieję, wszystko to, co musisz wiedzieć o bezpieczeństwie w Internecie, będąc jego statystycznym użytkownikiem. Zapraszamy do lektury.

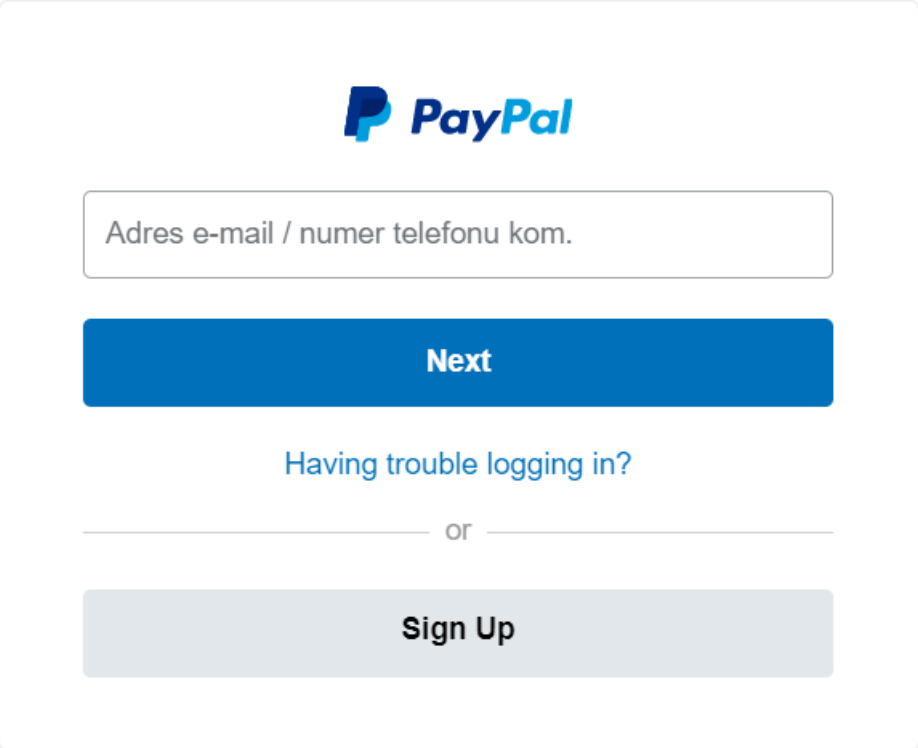
Co nam grozi w Internecie
Phishing

Phishing to jedna z najpopularniejszych obecnie metod oszustwa, która polega na podszywaniu się pod inną osobę lub instytucję w celu wyłudzenia danych. Najczęściej phishing przybiera formę informacji przesłanej za pośrednictwem maila lub SMSa. Fałszywe maile stylizowane mogą być na korespondencję pochodzącą od operatora telekomunikacyjnego, usługodawcy VOD (np. Netflixa), usług finansowych takich jak PayPal czy bank, serwisów aukcyjnych (OLX, Allegro) lub firm kurierskich (InPost, DHL, FedEx, i inne). Zazwyczaj będzie to informacja o zablokowaniu konta, lub możliwości zablokowania konta, brakach w płatności lub konieczności dopłaty nieznacznej kwoty, np. za przesyłkę, czy jakichś innych problemów z kontem lub usługą. Atakujący w taki sposób chcą nakłonić potencjalną ofiarę do kliknięcia w zawarty we wiadomości link, który prowadzić może do fałszywej strony logowania do banku, czy jakimś serwisie, fałszywej bramki płatności, strony logowania do Netflixa, czy Paypala. Uzyskane w ten sposób dane mogą spowodować, że atakujący przejmie za pomocą podanych mu przez ofiarę danych jej konto, a w efekcie narazi ją na straty nie tylko wizerunkowe, ale i finansowe.



Na grafice przedstawiono informację, którą ofiara otrzymała mailowo. Wiadomość sugeruje, że konto PayPal adresata zostało zawieszone i wymagane są dalsze czynności po zalogowaniu. Po kliknięciu w przycisk *log in* przekierowani zostajemy na stronę łudząco przypominającą stronę logowania usługi PayPal.

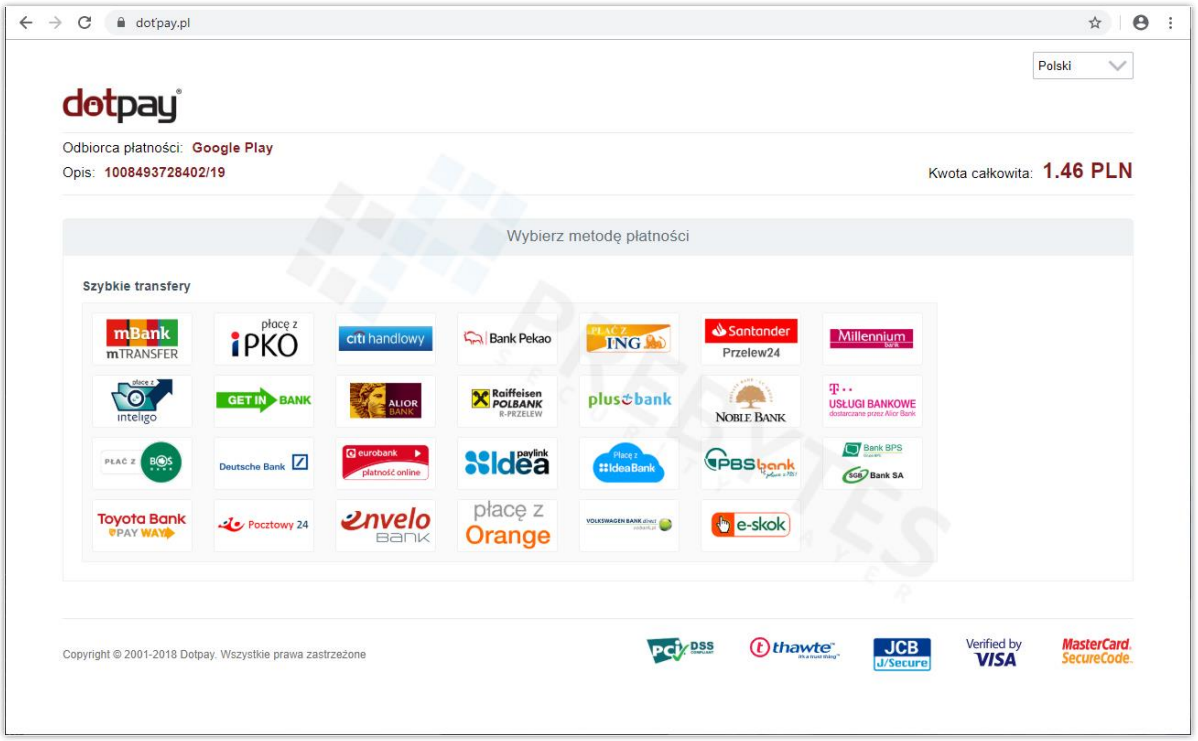
Na skróty: Jak chronić się przed phishingiem? Przede wszystkim loguj się jedynie na sprawdzonych stronach. Nie klikaj w linki we wiadomościach, które mogą budzić jakiekolwiek wątpliwości. Jeśli informacja twierdzi, że konto zostało zablokowane lub zawieszone zaloguj się bezpośrednio w serwisie i sprawdź to osobiście. Nie otwieraj również załączników z podejrzanych wiadomości.



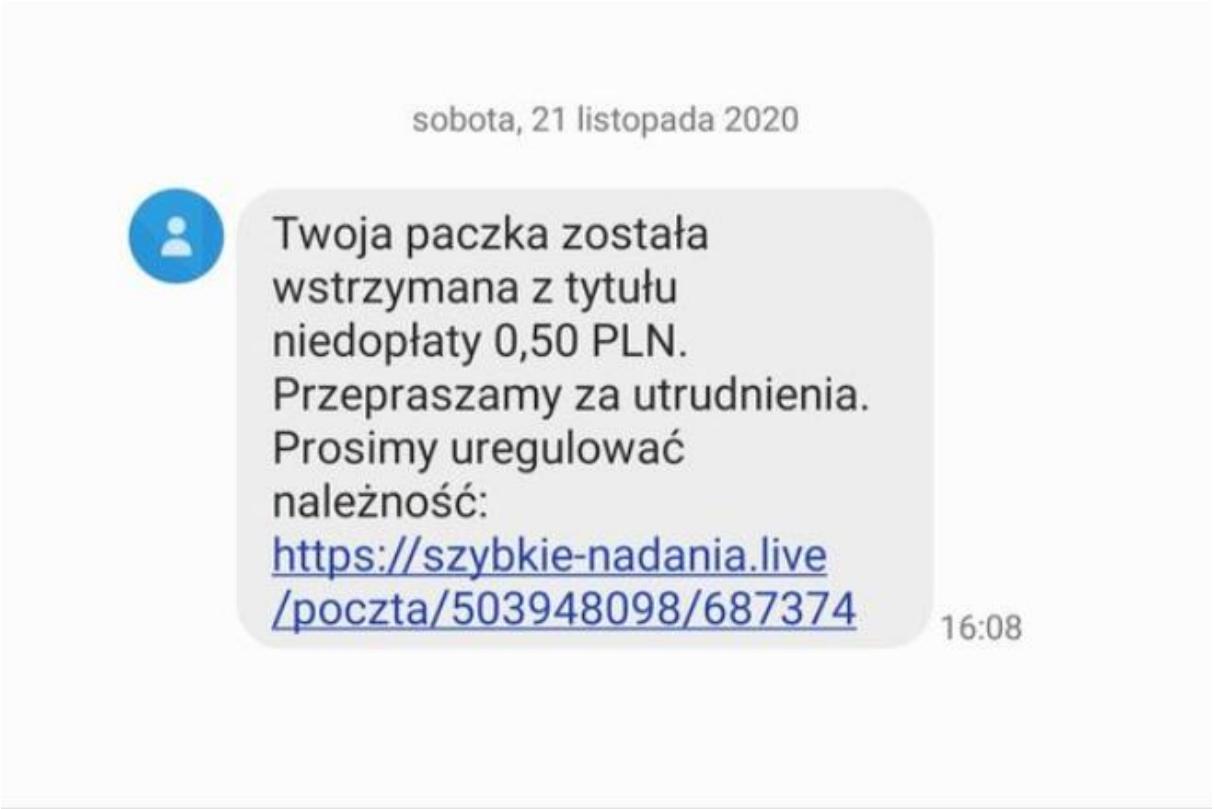
Po podaniu swoich danych atakujący przejmują konto ofiary. W przypadku posiadanych tam jakichś środków lub też podpiętej, aktywnej karty płatności należałoby liczyć się z ich utratą.

To, co upewnia nas o tym, że zostaliśmy skierowani na stronę próbującą wyłudzić dane jest jej adres. W tym przypadku jesteśmy pewni, że nie jest to prawidłowa strona logowania do PayPal – w pasku adresu powinien znaleźć się prawidłowy adres *paypal.com/pl/signin*. Oczywiście powyższy adres może przybierać różne formy, czasami od prawidłowego może różnić go jedynie drobny szczegół, np. literówka (*paipal.com*). Istnieje wtedy możliwość, że ofiara przegapi tę różnicę i również straci kontrole nad środkami i kontem.

Ze względu na rosnącą popularność Netflixa w Polsce usługa ta znalazła się również na celowniku przestępców. Schemat oszustwa jest identyczny, jak w poprzednim przykładzie. Otrzymujemy informację o zawieszeniu naszego konta. Po kliknięciu w link zawarty w wiadomości zostajemy przekierowani na fałszywą stronę logowania w serwisie. Jeśli podamy tam swoje dane stracimy konto.



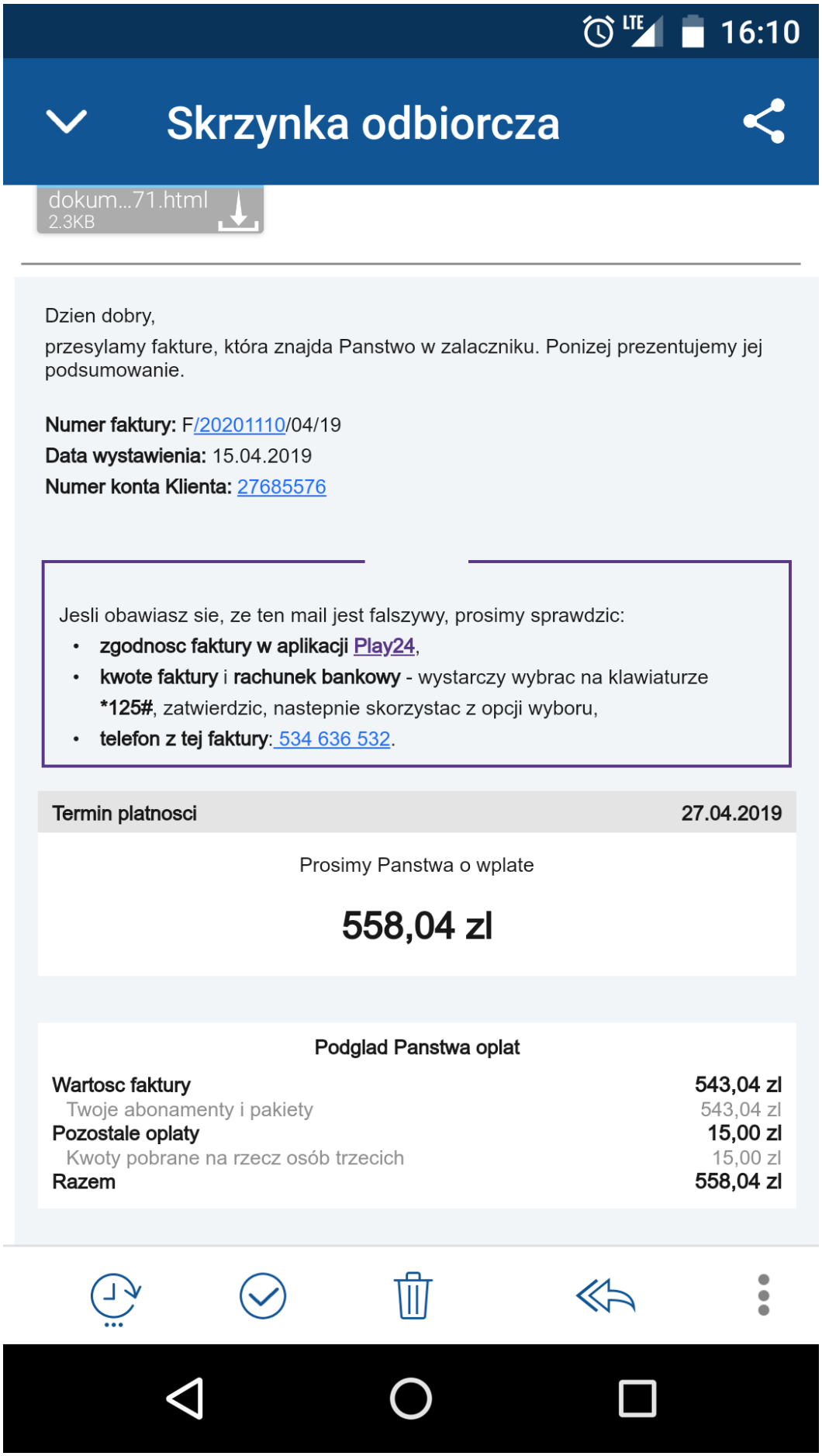
Ta wersja oszustwa bazuje na dopłacie do jakiejś usługi lub uregulowaniu należności. Ofiara otrzymuje wiadomość z prośbą o uregulowanie należności, zazwyczaj małej kwoty, żeby już na wstępie nie wzbudzać podejrzeń. Po kliknięciu w link do zapłaty widzimy bramkę płatności, łudząco podobną do bezpiecznej strony *dotpay*. Tylko drobny szczegół w adresie strony zdradza (znak ' pomiędzy wyrazami dot i pay), że nie jest to faktyczna bramka płatności, a próba wyłudzenia danych do logowania do bankowości internetowej. Ofiara wpisując dane na takiej stronie naraża się na utratę środków z konta. Po wpisaniu swoich danych do logowania atakujący będzie potrzebował jeszcze kodu autoryzacyjnego z wiadomości SMS. Jeśli ofiara w porę nie zorientuje się, że pada ofiarą oszustwa sama poda kod otrzymany SMSem. Przestępca w ten sposób doda swój rachunek bankowy do listy zaufanych odbiorców i przeleje wszystkie środki na kontrolowany przez siebie rachunek bankowy.



Opisywana wyżej metoda oszustwa występuje również w wariancie SMSowym. Otrzymujemy np. informację o drobnej zaległości, po kliknięciu w link zostajemy przekierowani do fałszywej bramki płatności. Pozostała część oszustwa pozostaje taka sama, jak opisywana powyżej.

Na skróty: Skąd przestępcy mają moje dane: email, numer telefonu?

Przestępcy pozyskują bazy danych potencjalnych ofiar na przeróżne sposoby. Część informacji udostępniamy sami, np. w mediach społecznościowych, ale większość pochodzi z dużych wycieków danych, np. ze sklepów internetowych w których mieliśmy konto, z for internetowych, czy innych serwisów w których założyliśmy konto, a z których dane następnie wyciekły. O wyciekach danych piszemy również w tym poradniku.



16:10

Skrzynka odbiorcza

dokum...71.html
2.3KB

Dzien dobry,

przesylamy fakture, która znajda Panstwo w zalaczniku. Ponizej prezentujemy jej podsumowanie.

Numer faktury: F/20201110/04/19
Data wystawienia: 15.04.2019
Numer konta Klienta: 27685576

Jesli obawiasz sie, ze ten mail jest falszywy, prosimy sprawdzic:

- **zgodnosc faktury w aplikacji Play24**,
- **kwote faktury** i **rachunek bankowy** - wystarczy wybrac na klawiaturze ***125#**, zatwierdzic, nastepnie skorzystac z opcji wyboru,
- **telefon z tej faktury**: 534 636 532.

Termin platnosci	**27.04.2019**

Prosimy Panstwa o wplate

558,04 zl

Podglad Panstwa oplat

Wartosc faktury	**543,04 zl**
Twoje abonamenty i pakiety	543,04 zl
Pozostale oplaty	**15,00 zl**
Kwoty pobrane na rzecz osób trzecich	15,00 zl
Razem	**558,04 zl**

Phishing może również, oprócz wyłudzania danych, próbować nakłonić ofiarę do pewnego zachowania. Powyższa grafika przedstawia kampanię cyberprzestępczą polegającą na rozsyłaniu fałszywych faktur za usługi telekomunikacyjne. W przeciwieństwie do opisywanych wyżej przypadków tutaj kwota faktura jest duża, co ma za zadanie przestraszyć potencjalną ofiarę i zmusić ją do otwarcia załącznika. W załączniku takiej złośliwej wiadomości ofiara może pobrać na swój komputer oprogramowanie, które niezauważenie będzie pracować w tle i w chwili np. wykonywania przelewów będzie podmieniać numery kont odbiorców na numer konta kontrolowanego przez atakujących.

Ofiarami tego typu oszustwa padli w 2015 roku urzędnicy z Jaworzna. Złośliwe oprogramowanie pracujące w systemie, który został zainfekowany po otwarciu takiej, lub podobnej, wiadomości i załącznika stracili podczas wykonywania przelewu prawie milion złotych. Pieniądze przelane zostały na numer konta, który został podmieniony w chwili wykonywania płatności właśnie przez tego typu oprogramowanie.

Żeby nie paść ofiarą phishingu należy z chłodną głową podchodzić do wszystkich wiadomości, które dostajemy na swoją skrzynkę mailową czy SMSową. Należy zastanowić się czego dana informacja może dotyczyć i czy jest wiarygodna. Jeżeli dotyczy blokady lub wymaga działania na koncie w serwisie z którego korzystamy nie należy klikać w linki zawarte w tej wiadomości. Należy przejść do danej usługi wpisując ręcznie w pasku przeglądarki adres i sprawdzić status swojego konta.

Nie należy również otwierać załączników podejrzanych wiadomości. Jeśli użytkownik nie ma pewności co do wiarygodności danej informacji najlepiej skontaktować się z osobą bardziej techniczną i poprosić o pomoc.

Co zrobić kiedy już padłem ofiarą phishingu?

Przede wszystkim, jeśli to tylko możliwe, należy udokumentować to, co się stało. W miarę możliwości należy wykonać zrzuty ekranów na których podawano swoje dane, zapamiętać domeny z którymi się łączono, nie usuwać wiadomości, które sugerowały dopłatę lub za pośrednictwem których przesyłane zostały linki. Poinformować należy koniecznie swój bank o tym, że zostało się okradzionym, a sprawę jak najszybciej zgłosić także policji. Należy również zgłosić od razu do swojego banku żądanie zwrotu pieniędzy.

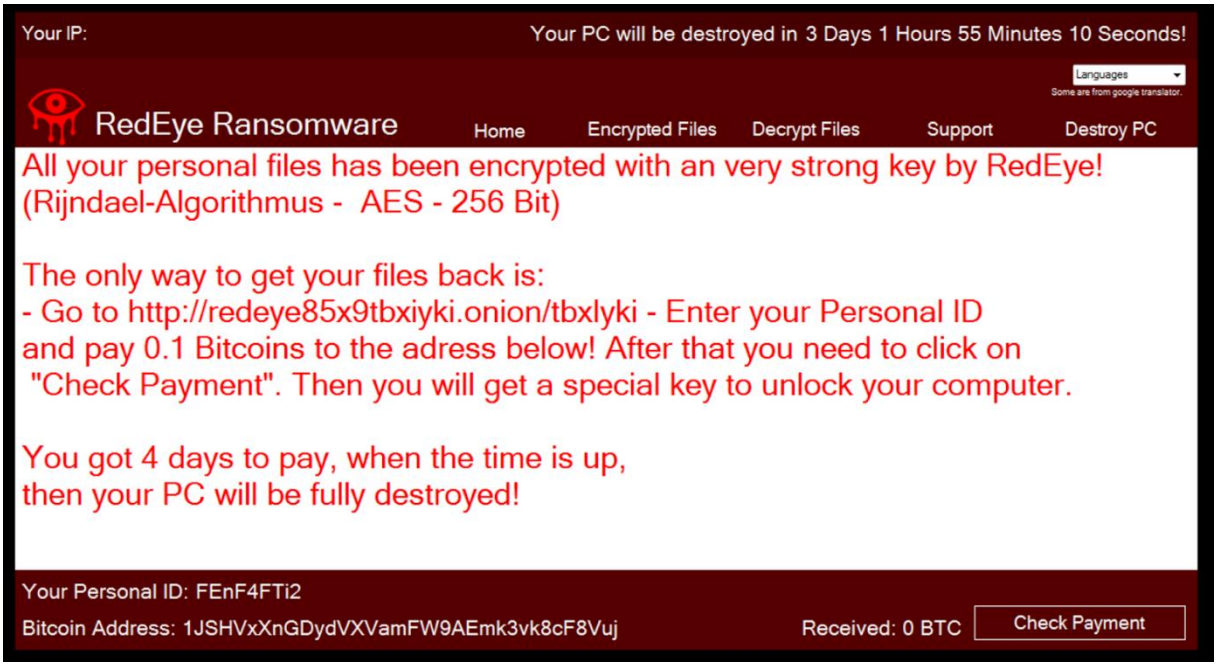
W dniu 20 czerwca 2018 roku w życie weszły przepisy ustawy z dnia 10 maja 2018 roku o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw, stanowiące implementację dyrektywy PSD II. Wprowadzone zmiany do ustawy o usługach płatniczych dotyczą między innymi zasad odpowiedzialności płatnika oraz sposobu postępowania dostawcy w przypadku wystąpienia nieautoryzowanej transakcji płatniczej. Celami dyrektywy PSD II – poza dostosowaniem przepisów do zachodzących na rynku zmian oraz ustandaryzowaniem przepisów regulujących rynek płatności – są także zapewnienie konsumentom większego bezpieczeństwa i zwiększenie zakresu ich ochrony.

Na skróty: Co to jest nieautoryzowana transakcja? To, zgodnie z art. 40, ust. 1 Ustawy o usługach płatniczych, transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą. Zgoda może dotyczyć także kolejnych transakcji płatniczych. Można więc uznać, że z nieautoryzowaną transakcją płatniczą mamy do czynienia w sytuacji, gdy płatnik nie wyraził na nią zgody.

Ransomware

Ransomware to oprogramowanie ograniczające dostęp (szyfruje dane na dysku) do systemu komputerowego i wymagające zapłacenia okupu, aby blokada została usunięta. Sposoby w jaki takie oprogramowanie może znaleźć się na komputerze ofiary i w efekcie zablokować dostęp do systemu są tożsame z tym, co opisane zostało w dziale Phishing tego poradnika. Może być to więc złośliwe oprogramowanie ukryte w załączniku do wiadomości i aktywujące się w systemie w momencie próby otwarcia. Ransomware może być jednak również ukryty w innych, pozornie niegroźnych programach, które np. ściągamy z sieci z niezbyt zaufanych źródeł. W naszym systemie to złośliwe oprogramowanie może pojawić się podczas próby uruchomienia pirackiej wersji gry lub innego oprogramowania pobranego z nieznanych nam serwerów lub z sieci torrent, lub też wymienianych pomiędzy użytkownikami plików na przenośnych nośnikach danych. Ransomware może okazać się szczególnie niszczycielski

jeśli nie posiadamy kopii zapasowych danych, które za sprawą takiego ataku zostały zaszyfrowane. Może się okazać, że jedynym ratunkiem jest sformatowanie dysku w swoim komputerze. Warto również pamiętać, że opisywane w tym poradniku zagrożenia typu phishing, czy ransomware (a także inne) dotyczą zarówno komputerów stacjonarnych, przenośnych, ale także urządzeń mobilnych.



Ekran po infekcji oprogramowaniem ransomware RedEye

Na skróty: Czy należy płacić okup za odzyskanie swoich danych? Takie rozwiązanie nigdy nie jest zalecane. Ofiara nie ma pewności czy jej pliki za pomocą przesłanego klucza zostaną odszyfrowane. Ransomware może również zawierać błędy, które spowodują, że pliki na komputerze ofiary zostaną uszkodzone. Zapłacenie okupu skutkuje również większą liczbą infekcji.

Czasem w dostępie do zaszyfrowanych plików i zablokowanych systemów, bez konieczności płacenia, pomaga inicjatywa *NoMoreRansom.org*. W serwisie tym stworzono repozytorium kluczy i aplikacji, które pozwalają (czasem) odzyskać dane zaszyfrowane przez różnego rodzaju oprogramowania ransomware.

Ataki ransomware są szczególnie uporczywe dla wszelkich organizacji: biznesu czy też wszelkiego rodzaju instytucji publicznych. Poważny atak tego typu sparaliżował pod koniec 2020 roku hrabstwo Delaware w Pensylwanii. Ataku mieli dokonać cyberprzestępcy kryjący się pod nazwą *DoppelPaymer*, a urzędnicy okręgu administracyjnego w Pensylwanii, odpowiadającemu polskiemu powiatowi, zmuszeni byli do zapłaty 500 tysięcy złotych okupu w zamian za odzyskanie kontroli nad częścią systemu informatycznego. Atak złośliwym oprogramowaniem, w skrajnym przypadku, może doprowadzić również do śmierci ludzi. We wrześniu 2020 roku ze szpitala w Dusseldorfie odesłano kobietę, do placówki oddalonej o 30 km. Nie udzielono jej pomocy ze względu na awarię systemu informatycznego, koniecznego do diagnozy, spowodowanego infekcją oprogramowaniem typu ransowmware. Kobieta w trakcie transportu do kolejnej placówki zmarła. Szpital w Dusseldorfie najprawdopodobniej nie był głównym celem ataku przestępców. Takim miała być uczelnia Heinrich Heine University Düsseldorf, która jednak połączona jest siecią z placówką zdrowia. Zainfekowanie było skutkiem luki w popularnym, komercyjnym oprogramowaniu. Zaraz po tym jak do sprawy weszła policja szpital otrzymał od przestępców klucze deszyfrujące.

Jednym z najgłośniejszych przykładów ataku ransomware'owego z ostatnich miesięcy był paraliż firmy Garmin. Amerykańska firma z branży odbiorników GPS oraz urządzeń wereables została w sierpniu 2020 roku zaatakowana szkodnikiem *WastedLocker*. Stanęła cała sieć firmy oraz linia produkcyjna. Część zapisanych danych w Garmin Connect zniknęła bezpowrotnie. Pierwsze usługi Garmina wróciły do życia dopiero po kilku dniach. *SkyNews* donosił wtedy, że Garmin najzwyczajniej w świecie poddał się przestępcom i zapłacił okup. Pierwotnie, według doniesień *BleepingComputer*, miał wynosić on 10 milionów dolarów. Zapłacona przez Garmin kwota nie została ujawniona, ale *SkyNews* pisał o kilku milionach dolarów. Garmin jest liderem w jakości sygnału satelitarnego oraz producentem nawigatorów do transportu powietrznego, drogowego, motorowego i wodnego. Z urządzeń i usług amerykańskiej firmy korzysta również wojsko. Brak aktualizacji wielu usług oraz możliwości synchronizacji urządzeń w tym przypadku wpływała bezpośrednio na bezpieczeństwo narodowe.

Aby ustrzec się przed atakiem ransomware należy przestrzegać kilku podstawowych zasad. Nie otwierać załączników z wiadomości od nieznanych nadawców, nie uruchamiać programów pochodzących z nieznanego źródła. Ważnym elementem cyberhigieny w tym zakresie jest używanie jedynie legalnego oprogramowania oraz regularne aktualizowanie systemu operacyjnego oraz wszystkich zainstalowanych w systemie programów.

Socjotechniki

Kevin Mitnick, nazywany najbardziej znanym hakerem świata, napisał w swojej książce *Sztuka podstępu*, że *łamał ludzi, nie hasła*. Stąd też miejsce w tym poradniku dla socjotechniki, nazywanej czasem inżynierią społeczną. Socjotechnika to pojęcie określające techniki manipulacji człowiekiem. Krótko i zwięźle można powiedzieć, że socjotechnik kieruje swoją ofiarą tak, z wykorzystaniem dostępnej mu wiedzy i narzędzi, aby ta zachowywała się i robiła to, na czym zależy atakującemu. W opisywanych dotychczas przykładach phishingu i ransomware przestępcy również wykorzystują te techniki. Wysyłając masowo wiadomości o blokadzie konta w jakiejś usłudze, dopłacie małych kwot z zachętą do natychmiastowego opłacenia, czy też fałszywą fakturą na dużą kwotę liczą, że ofiara ze strachu przed utratą pracy, z roztargnienia (bo to mała kwota, a przesyłka jest w drodze), czy też ze strachu przed dużym rachunkiem zechce się od razu dowiedzieć o co chodzi i kliknie zainfekowany załącznik lub też opłaci zaległość i tym samym uzyskają nad nimi kontrolę. Złośliwe maile rozsyłane są jednak masowo, z nadzieją, że pewien ich procent trafi do faktycznych użytkowników danej usługi. Istnieje jednak wersja ataku phishingowego w której atakujący zna swoją ofiarę. W takim przypadku mówimy o ataku nazywanym *spear phishing* (phishingu ukierunkowanym). Atak taki poprzedza niekiedy wielomiesięczny rekonesans dotyczący ofiary. Przestępca dowie się jak ofiara ma na imię, czy ma i jak mają na imię jej rodzice, dowie się czy ofiara ma jakieś zwierzątko domowe, czym się

interesuje, gdzie mieszka i gdzie lubi chodzić i jak spędzać czas. W tym procesie nie ma informacji bez znaczenia. Wszystkie mogą być później wykorzystane w trakcie ataku, aby zdobyć przychylność ofiary, jej zaufanie i stworzyć wrażenie *dobrego znajomego*, czy też współpracownika *zza ściany*. Zmanipulowana ofiara będzie w ten sposób podatniejsza na kliknięcie w złośliwy link, uruchomienie oprogramowania, które nigdy nie powinno trafić do służbowego systemu, czy też podania informacji, które nigdy nie powinny być udostępnione komuś z zewnątrz. Jednym z wariantów takiego ataku jest *business email compromise*. Jest to atak polegający na skierowaniu korespondencji do działu finansowego firmy, podając się za kontrahenta, dostawcę, czy wierzyciela lub też szefa, członka zarządu czy inną wysoko postawioną w hierarchii firmy osobę. Odbiorca ma odnieść wrażenie, że sprawa jest pilna. Zazwyczaj atak polega na nakłonieniu ofiary do zmiany numeru konta bankowego kontrahenta na ten podany przez atakującego. Dla przestępcy wszystkie zdobyte wcześniej informacje na temat ofiary mogą być przydatne. Niejednokrotnie dzwoni do swojej ofiary i usypia jej czujność wypytując np. o szczegóły z życia prywatnego, a następnie, już po zbudowaniu wstępnego zaufania, przechodzi do ataku w którym informuje, że wszystkie kolejne przelewy muszą być wykonywane na nowy numer konta bankowego.

Ofiarą takiego oszustwa padła jedna ze spółek Polskiej Grupy Zbrojeniowej. Zajmująca się handlem bronią spółka Cenzin otrzymała od jednego z kontrahentów maile, a proces oszustwa wyglądał dokładnie tak, jak opisywany powyżej. Spółka straciła ok. 4 milionów złotych. Atakujący w trakcie takiego przestępstwa mogą posługiwać się również tzw.

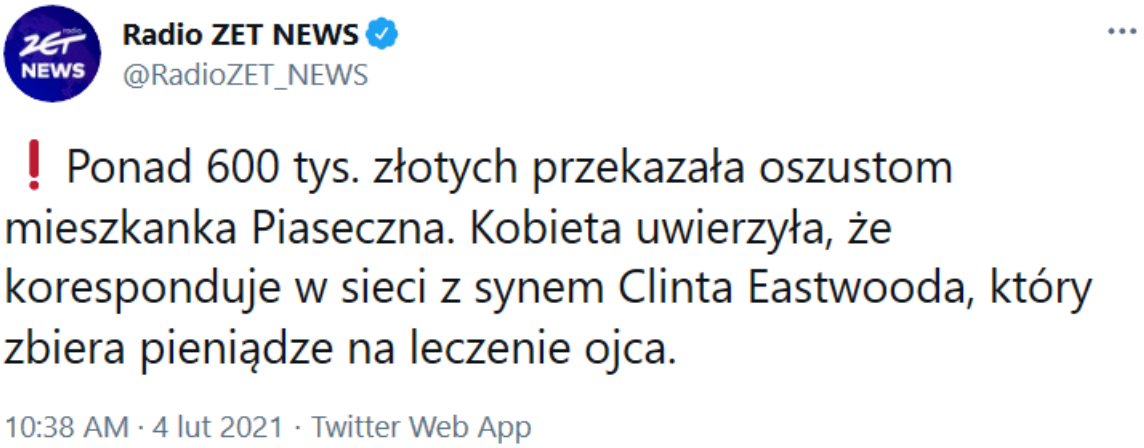
spoofingiem, czyli symulować kontakt z zaufanego źródła (adresu email lub numeru telefonu).

Na skróty: Jak zachować się w przypadku phishingu ukierunkowanego?

Jeśli ktoś podający się kontrahenta, współpracownika czy przełożonego kontaktuje się w niecodziennej sprawie, np. wykonania przelewu na inne niż dotychczas rachunki bankowe, zachowajmy czujność. Osoba odpowiedzialna za płatności powinna zweryfikować te informacje bezpośrednio u źródła. Spoofing, czyli podszywanie się pod jakiś adres email lub numer telefonu działa tylko w jedną stronę. Oddzwaniając pod znany numer telefonu może okazać się, że jego właściciel w ogóle się z nami nie kontaktować, a cała sprawa jest próbą oszustwa.

Ofiarą socjotechniki może paść każdy zwykły użytkownik Internetu. Znane są oszustwa w których atakujący na portalach społecznościowych wyszukują np. samotne kobiety i pod pretekstem nawiązania znajomości lub związku manipulują swoją ofiarą w taki sposób, aby ta przekazała mu np. jakąś określoną sumę pieniędzy, pod jakimkolwiek pretekstem.

Kobieta z Chełmna uwierzyła, że pisze do niej znany amerykański aktor Will Smith. 35 latka przekazała oszustowi 45 tysięcy złotych, bo uwierzyła, że ten chce przenieść się do Polski, a pieniądze te są potrzebne na opłacenie paczki z kosztownościami i dokumentów. Do podobnych oszustw dochodzi niemal codziennie.



Jeden z najnowszych przykładów oszustwa

Załóżmy hipotetyczną sytuację w której poprzez komunikator pisze do nas dobry znajomy, który prosi o pożyczkę (np. 500 złotych), ponieważ utknął na autostradzie i pieniądze te potrzebne są mu na opłacenie lawety i holowanie samochodu. Ma to być przelew natychmiastowy, albo kod BLIK. Jeżeli odpowiemy na taką prośbę bez weryfikacji to najpewniej stracimy te pieniądze. Oszuści przejmują konta na portalach społecznościowych w sposób opisywany w poprzednich działach tego poradnika (np. w sposób phishingu), a następnie próbują oszukać osoby znajdujące się na liście znajomych ofiary. Oszuści mogą również sklonować konto jakiejś osoby, tworząc profil z takim samym imieniem i nazwiskiem, pobierając i dodając do profilu takie same zdjęcia, jak zdjęcia ofiary i w ten sposób próbować oszukać osoby znajdujące się na liście znajomych. Przejęty profil ofiary może też np. posłużyć do wystawiania różnych przedmiotów w facebookowej usłudze *Marketplace*. Oszustwa dokonane w ten sposób obciążać będą w pierwszej kolejności prawowitego właściciela profilu.

Wycieki danych i kradzież tożsamości

Czytelnik zapoznając się z powyższym poradnikiem zapewne zastanawia się skąd przestępcy, a każdy z nas spotyka się z próbami oszustwa czy ataku niemal codziennie, ma dane swoich ofiar – adresy email, numery telefonów, czasem numery PESEL, czy dane osobowe, w tym te podlegające szczególnej ochronie. Odpowiedź jest bardzo prosta. Z wycieków danych. Korzystając na co dzień z przeróżnych serwisów i usług internetowych pozostawiamy swoje dane w każdej z nich. Zwykło się mówić, że pytaniem nie jest to, czy z danej usługi internetowej nasze dane wycieką. Pytaniem jest jedynie kiedy to nastąpi. W 2018 roku doszło do poważnego wycieku danych ze sklepu internetowego *Morele.net*. Szacowano, że dane, które dostały się do sieci dotyczyły ok. 2,5 miliona osób korzystających z tego sklepu. Urząd Ochrony Danych Osobowych wszczął postępowanie, które zakończyło się dużą, jak na polskie warunki, karą finansową w wysokości 2,8 miliona złotych. To najwyższa tego typu kara nałożona dotychczas przez UODO. Dane, które wówczas wyciekły niemal od razu posłużyły przestępcom do kampanii phishingowych. Atakujący rozsyłali smsy informujące o brakującej wpłacie 1 zł, wskutek czego rzekome zamówienie nie może zostać zrealizowane, prosząc jednocześnie o uzupełnienie tej niewielkiej kwoty. Link w smsie prowadził oczywiście do fałszywej strony płatności, dzięki której oszuści uzyskiwali dostęp do kont bankowych i smsów autoryzujących transakcje swoich ofiar.

Na skróty: Czy da się zabezpieczyć przed wyciekiem danych? Nie da się, bo to nie zależy od nas. Jako użytkownik możemy jednak minimalizować ryzyko i nie rejestrować się do usług, których tak naprawdę nie potrzebujemy. Możemy również nie podawać swoich danych tam, gdzie nie jest to absolutnie potrzebne. Możemy również żądać usunięcia naszych danych osobowych z jakiegoś zbioru. Mówi o tym art. 17 RODO, usunięcie może nastąpić jednak pod pewnymi warunkami.

Informacja o kradzieży danych osobowych części klientów operatora Virgin Mobile, podana w Święta Bożego Narodzenia 2019 roku, wywołała ponowną lawinę komentarzy w sieci dotyczącą ochrony danych osobowych i tego, co z tak pozyskanymi danymi może zrobić przestępca. Virgin Mobile Polska poinformował swoich klientów, że infrastruktura firmy padła ofiarą ataku w wyniku którego wyciekły dane klientów usługi prepaid. Sprawa ma dotyczyć około 12 procent wszystkich klientów tej usługi, a dane o których

mowa to imię, nazwisko, numery PESEL lub numery dokumentu tożsamości. Wyciek związany był z usługą przeznaczoną do generowania potwierdzeń rejestracji prepaid przez punkty POS. Do ataku miało dojść w dniach 18 - 22 grudnia 2019 roku, a operator wykrył wyciek 22 grudnia. Od tego momentu więc dane części abonentów Virgin znajdują się w rękach przestępców i mogą oni zrobić z nimi, co chcą.

Mogą np. wziąć kredyt na dane osobowe ofiary. Niestety zaciągnięcie kredytu na czyjeś dane jest wciąż w Polsce za łatwe, choć oczywiście trochę w tej sprawie się zmienia i firmy pożyczkowe, a także banki mają, i ciągle udoskonalają, własne formy zabezpieczeń. I trzeba w tym miejscu powiedzieć także, że numery PESEL, nazwiska, adresy zamieszkania, przeróżne dane dotyczące dokumentów tożsamości wcale nie muszą pochodzić tylko z wycieków - jeśli przestępca wykaże się odrobiną inwencji i cierpliwości może te dane zebrać z ogólnodostępnych źródeł, takich jak Facebook, Google czy przeróżne rejestry dostępne w sieci.

Jak zabezpieczyć się przed kradzieżą tożsamości

Jest kilka możliwości dla osoby fizycznej. Po pierwsze usługa Bezpieczny Pesel. Jak czytamy na stronie *bezpiecznypesel.pl* serwis został uruchomiony w 2017 roku we współpracy CRIF Sp. z o.o. z Polskim Związkiem Instytucji Pożyczkowych, jako pomysł na edukowanie społeczeństwa w zakresie bezpieczeństwa finansowego i przeciwdziałanie zjawisku nadmiernego zadłużenia Polaków. Twórcy usługi podają na swojej stronie, że od momentu jej uruchomienia zapobiegli wyłudzeniom na łączną kwotę ponad 20 milionów złotych.

Serwis działa w bardzo prosty sposób – zastrzegamy swoje dane na stronie usługi w dwóch konkretnych sytuacjach:

- chcemy chronić numer PESEL przed kradzieżą tożsamości, a co za tym idzie zapobiegać możliwości wyłudzania pożyczek w instytucjach pożyczkowych – zastrzegamy numer PESEL
- tracimy dokumenty, powiadamiamy policję, zgłaszamy informację o utracie dokumentów – zastrzegamy numer PESEL.

Zastrzegane dane trafiają do Systemu CRIF (baza danych) i służą weryfikacji konsumentów zaciągających pożyczki. Raz zastrzeżony numer PESEL jest chroniony w takiej bazie do czasu, kiedy samodzielnie dokonasz cofnięcia zastrzeżenia numeru PESEL lub zgłoszenia utraty dokumentów. Usługa Bezpieczny Pesel jest bezpłatna, ale, żeby z niej skorzystać, czyli, żeby nasz PESEL mógł zostać objęty ochroną musimy na stronie usługodawcy potwierdzić swoją tożsamość, czyli przekazać mu swoje dane, łącznie z numerem i skanem dowodu tożsamości, numerem PESEL i adresem zamieszkania. Podobne usługi świadczy również Biuro Informacji Kredytowej. BiK dostarcza rozwiązanie tzw. Alertu BiK, czyli powiadomienia właściciela PESELu o tym, że ktoś próbuje użyć jego danych do wzięcia kredytu, czy pożyczki lub kiedy pojawi się zapytanie w Rejestrze Dłużników BIGInfoMonitor. Usługa Aleru BiK jest płatna, ale abonament roczny w którym uzyskujesz sam Alert, możliwość zastrzeżenia dokumentu oraz zastrzeżenia kredytowego to jedynie 24 złote. Pakiet o wartości 99 złotych na rok daje ci dodatkową możliwość pobrania 12 raportów BiK, ta opcja jest również wzbogacona o Wskaźnik BiK.

Z innych, dostępnych usług warto wymienić jeszcze *ChronPESEL.pl*. Tu mamy do wyboru trzy opcje abonamentowe - jest to bowiem także usługa płatna i jest już odrobinę drożej. Najtańszy pakiet to 175 złotych rocznie, a otrzymujemy w nim możliwość sprawdzenia kto w ciągu ostatnich 12 miesięcy wykorzystywał nasz PESEL, możliwość sprawdzenia czy jesteśmy wpisani do Krajowego rejestru Długów, otrzymujemy usługę powiadamiania o użyciu naszego PESELa oraz powiadomienie o dopisaniu nas do Krajowego rejestru Długów.

Co zrobić, kiedy stałeś się już ofiarą kradzieży tożsamości

Warto również wspomnieć, co należałoby zrobić w przypadku, kiedy ktoś wziął już pożyczkę na nasze dane. Oczywiście, przede wszystkim, powiadamiamy o oszustwie policję, informujemy o tym także instytucję pożyczkową w której zostało zaciągnięte zobowiązanie na nasze dane - jeśli wiemy w której. Pamiętamy o możliwości zgłoszenia sprzeciwu na decyzję e-Sądu, wtedy taka sprawa trafia do sądu tradycyjnego w którym wnosimy o sprawdzenie autentyczności podpisów na umowach pożyczkowych i wszelkich innych dowodów związanych ze sprawą. Pamiętamy również o tym, że w przypadku, kiedy w ogóle nie wiedzieliśmy o wydanym przez e-Sąd nakazie zapłaty możemy złożyć wniosek o przywrócenie terminu na złożenie sprzeciwu. Do naszej dyspozycji pozostają także prawnicy Polskiego Związku Instytucji Pożyczkowych z którymi możemy skontaktować się poprzez infolinię 800 706 813.

Fałszywe sklepy online

Coraz więcej osób korzysta z zakupów w sieci. Tocząca się pandemia jeszcze to zjawisko spotęgowała. Tymczasem już w 2018 roku Narodowe Centrum Cyberbezpieczeństwa ostrzegało o wzmożonym procederze oszustw za pomocą fałszywych sklepów internetowych. Nieprawdopodobna okazja. Buty, które oryginalnie sprzedawane są za około 900 złotych w promocyjnej cenie 360 zł? To jedna z przesłanek, która powinna uruchomić w naszej głowie czerwoną, ostrzegawczą lampkę podczas robienia zakupów w sieci. Takie okazje się po prostu nie zdarzają i warto zdać sobie z tego sprawę, zanim jeszcze stracimy swoje pieniądze. Dziś w Internecie bowiem aż roi się od fałszywych sklepów internetowych, które kuszą wielkimi zniżkami, bonami i promocjami, ale jedyne czego możemy się spodziewać po przesłaniu pieniędzy to ból głowy i żal po ich stracie. Plagą obecnie jest również tzw. *dropshipping*, czyli model logistyczny sprzedaży w sieci polegający na przeniesieniu procesu wysyłki towaru na dostawcę. Rola sklepu w tym przypadku sprowadza się do zbierania zamówień i przesyłania ich do dostawcy, który realizuje wysyłkę towaru do klienta. Teoretycznie nic strasznego, w praktyce jednak oznacza to całkowity brak odpowiedzialności sklepu za wysyłkę towaru, a w większości przypadków najzwyczajniej pod tym modelem kryje się zwykłe oszustwo. W najlepszym przypadku za wysłane pieniądze otrzymamy nic nie warte, tanie podróbki z Chin.

Na skróty: Jak rozpoznać fałszywy sklep internetowy? Naszą uwagę powinny zwrócić znacznie niższe ceny, niż faktyczna wartość towaru w innych miejscach. Brak kontaktu z obsługą sklepu, brak adresu lub adres nieistniejący, brak danych firmy, domena zarejestrowana niedawno, brak możliwości płatności kartą – to czynniki, które powinny wzbudzić naszą nieufność.

To, co powinno w przypadku sklepu internetowego wzbudzić naszą nieufność to brak praktycznie jakichkolwiek danych firmy do której należy sklep. Próżno na takich stronach szukać nr KRS czy REGON (oczywiście zdarzają się takie, które te dane podają, wtedy należy je rzetelnie sprawdzić). Adres sklepu również zazwyczaj nie jest podany, a jeśli jest, to chwila spędzona z Google daje nam odpowiedź, że pod podanym adresem nie mieści się żadna firma. W dziale kontakt sklepu nie istnieje nic, oprócz adresu email z którego jednak nikt na stawiane pytania i wątpliwości nie odpowiada. Domena pod którą znajduje się fałszywy sklep zazwyczaj zarejestrowana została bardzo niedawno, a sam sklep to gotowe oprogramowanie np. na silniku Shoper, który uruchomić może każdy za niewiele ponad 30 złotych w abonamencie miesięcznym.

Jak wyglądają zakupy w takim sklepie?

W zasadzie standardowo, po wybraniu interesującego nas przedmiotu, ewentualnego rozmiaru, koloru i innych detali przechodzimy do finalizacji zamówienia. Towar możemy zakupić z rejestracją/ logowaniem lub bez. Przechodząc do płatności okazuje się, że jedyną jej formą jest standardowy przelew, czyli na podane dane musimy sami, z własnego konta, dokonać

przelewu. Dlaczego to takie ważne? Dlatego, że przelewając w ten sposób pieniądze nie mamy praktycznie żadnych szans na ich odzyskanie. Wyśledzenie faktycznego odbiorcy pieniędzy także będzie niezwykle trudne bo konto na które klienci przelewają środki za swoje zakupy najprawdopodobniej założone zostało na słupa lub nieświadomą osobę, której skradziono tożsamość. Legalne sklepy internetowe udostępniają swoim klientom kilka form płatności, w tym płatność kartą, która, ze względu na funkcję *chargeback*, jest najpewniejszą formą płatności w sieci. Chargeback to po polsku obciążenie zwrotne. Najprościej mówiąc, jest to mechanizm, który ma na celu ochronę kupujących. W sytuacji, jeżeli po otrzymaniu zamówienia klient stwierdzi, że produkty lub usługi są z nim niezgodne, może zażądać zwrotu pieniędzy właśnie w formie chargebacku.

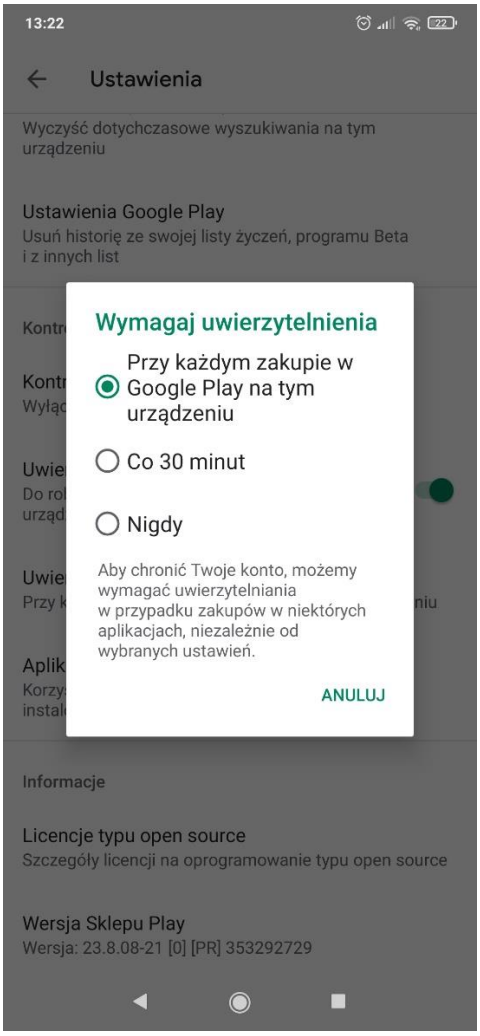
Dziecko w Internecie

Wszystkie zagrożenia opisywane w tym poradniku mogą dotyczyć również dzieci, które są przecież aktywnymi uczestnikami życia w sieci. Korzystają one jednak z Internetu nieco inaczej, a więc i zagrożenia płynące z tego faktu będą nieco inne. Dziecko nie pracuje za pomocą komputera w biurze, a więc nie może być narażone np. na atak typu *business email compromise*. Dzieci robią natomiast zakupy w sieci, a więc już niebezpieczeństwo tego, że padną ofiarą oszustwa w fałszywym sklepie internetowym jest dużo większe. Tym bardziej, że nie są one wyposażone jeszcze w tak dobry instynkt jak dorośli, nie posiadają również tak dużego doświadczenia

życiowego, żeby móc swobodnie i samodzielnie rozpoznać zagrożenie. Najmłodsi użytkownicy sieci są jednak równie często narażeni na ataki phishingowe, jak osoby dorosłe. Te, jeśli idzie o mechanizm, są takie, jak już opisywano, ale otoczenie oszustwa może być inne. Dzieci chętnie korzystają z usług gier online, które działają na zasadzie *free to play*. Taka usługa pozwala zainstalować i grać w grę bez opłat, ale dodatkowe wyposażenie w grze lub jakieś specjalne umiejętności postaci są już płatne. I takie konta dzieci, które mają jakąś wartość, posiadane przedmioty lub całe konta można odsprzedać, są właśnie na celowniku internetowych oszustów. Ci polują na posiadaczy kont wewnątrz gier lub też na komunikatorach i chatach przeznaczonych dla graczy, np. Discord. Pod pretekstem darmowej aktualizacji, jakiegoś bonusa czy prezentu, wyłudzają od dzieci dane logowania, a następnie sprzedają (kradną) konta lub poszczególne przedmioty w grach. Specjaliści do spraw cyberbezpieczeństwo już w 2015 roku alarmowali, że miesięcznie w usłudze Steam hakowanych jest ponad 77 tysięcy kont użytkowników. Sam Steam w 2011 roku wprowadził możliwość handlu przedmiotami posiadanymi na swoim koncie (Steam Trading).

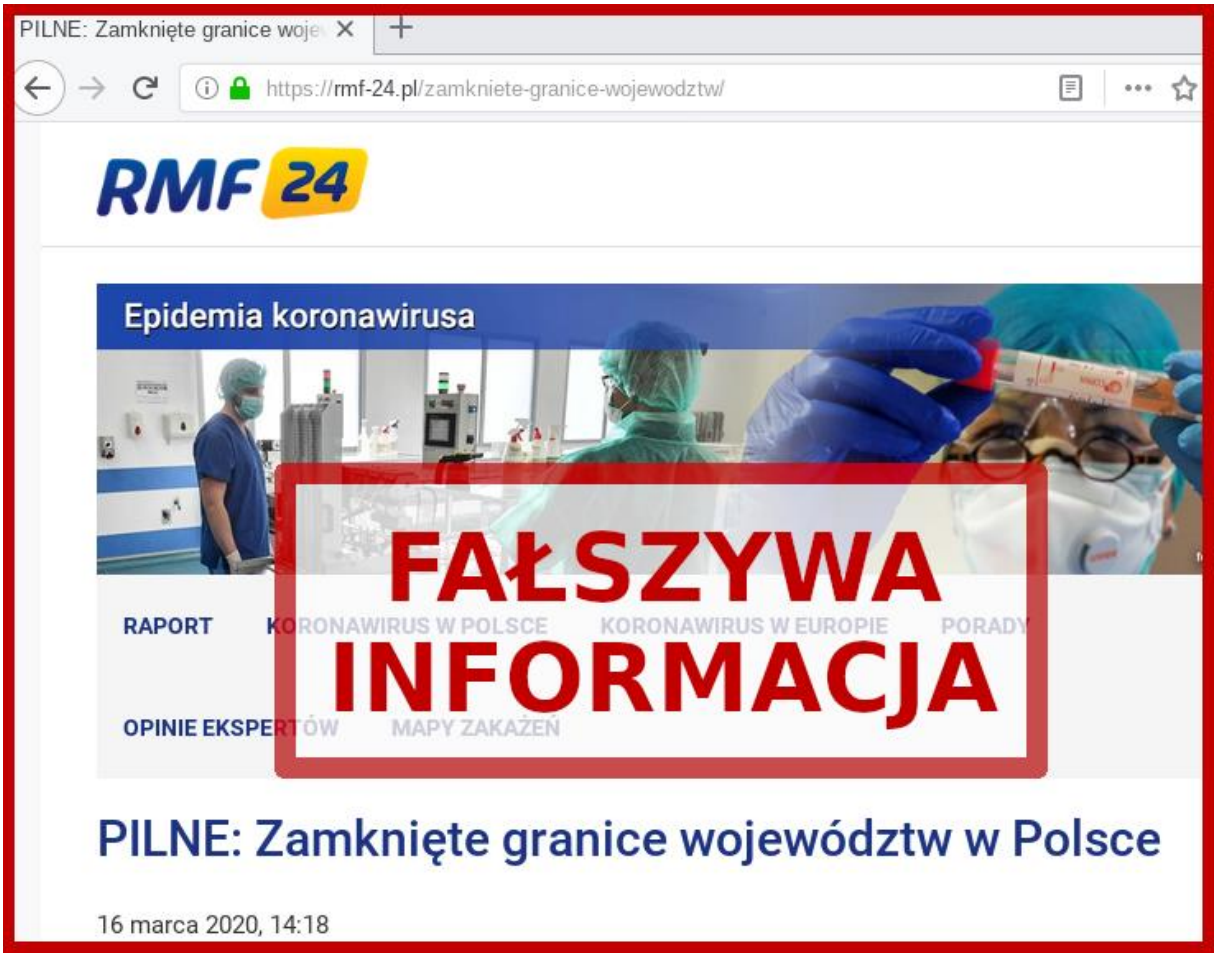
Zakupy aplikacji lub zakupy wewnątrz aplikacji czy gier często dokonywane są za pomocą środków z kont rodziców. Warto zainteresować się więc tym, jakie sumy dziecko wydaje na cyfrowe przedmioty, ustawić stosowne limity i ustalić zasady. 11 latka z Wielkiej Brytanii wydała z konta swojego ojca (w przeliczeniu) 23 tysiące złotych na różne przedmioty w bardzo popularnej wśród dzieci grze Roblox. Dzieci niejednokrotnie wykorzystują również sprzęt rodziców do zabawy. Może to być służbowy laptop, czy prywatny smartfon. Nie zawsze pobrane oprogramowanie jest tym, czym wydaje się być. Wewnątrz aplikacji, które z pozoru wydają się

niegroźne, może zaszyte być złośliwe oprogramowanie, które w odpowiednim momencie będzie np. w stanie wykraść dane logowania do bankowości internetowej lub inne dane znajdujące się na urządzeniu. Tego typu niespodzianki mogą się zdarzyć również w oficjalnym sklepie z oprogramowaniem na system Android, w Google Play. Urządzenia mobilne również służą do zabawy i również możliwe jest dokonywanie za ich pomocą płatności. Domyślnie w systemach Android, przy każdym zakupie, istnieje potrzeba dodatkowego uwierzytelnienia. Dzieci potrafią być jednak w tej kwestii niezwykle kreatywne wyłączając zabezpieczenia lub też, znając kod urządzenia, same, nieświadome konsekwencji, wprowadzają je i w ten sposób autoryzują transakcje.



O co chodzi z zielonymi kłódkami

Niejednokrotnie spotkać można się z twierdzeniem, że tzw. *zielona kłódka* przy adresie strony oznacza, że jest ona bezpieczna. Tego typu twierdzenia spotkać można również na niektórych szkoleniach z cyberbezpieczeństwa. To jednak zbyt wielkie uproszczenie wprowadzające w czytelniku, czy osobie szkolonej, poczucie, że sama obecność certyfikatu SSL gwarantuje bezpieczeństwo. Tak nie jest.



Choć podana strona legitymuje się *zieloną kłódką* to nie jest witryną radia RMF i powstała do wyłudzania danych

Żeby przekonać się o tym dlaczego zielona kłódka automatycznie nie oznacza bezpieczeństwa musimy sobie zdefiniować najpierw czym tak naprawdę jest certyfikat SSL. Posiadanie go na stronie internetowej oznacza jedynie, że dane przesyłane z urządzenia na którym pracujemy do serwera i w drugą stronę są szyfrowane - czyli, nie można ich podsłuchać (zastosować np. ataku *man-in-the-middle*). Certyfikat SSL gwarantuje także konsystencję danych oraz potwierdzają, że połączyliśmy się z tym, kim chcieliśmy. I to tutaj pojawia się problem, bo certyfikaty SSL występują w trzech rodzajach.

- **Domain validation** - dostawca certyfikatu sprawdza jedynie, czy domena na której znajduje się certyfikat jest własnością tego, kto certyfikat instaluje. Nic poza tym. Taki certyfikat można otrzymać za darmo i oprócz szyfrowanego połączenia z serwerem docelowym, który przecież może być pod kontrolą oszusta, i odwrotnie, nie gwarantuje niczego więcej. To na takie certyfikaty i mityczne zielone kłódki nabierają się najczęściej ofiary wszelkich phishingów i scamów.
- **Extended validation** - to certyfikat rozszerzony. Zamiast zielonej kłódki przy adresie strony widnieje zielony pasek z nazwą firmy do której należy certyfikat.
- **Organization validated** - to certyfikat wymagający od właściciela strony najwięcej zachodu, a tym samym uznawany jest za najbardziej bezpieczny. W tym przypadku właściciel musi dowieść, że nie tylko jesteś właścicielem danej domeny, ale także właścicielem firmy na którą się powołuje. Jeśli więc certyfikat wystawiony jest na Bank Polska Kasa Opieki S.A. to można mieć pewność, że łączy się ze stroną należącą do banku PeKaO S.A.

Wszystkie te rzeczy możesz łatwo sprawdzić na pasku adresu przeglądarki. Warto w tej kwestii zachować czujność.

Jak się zabezpieczać
Polityka haseł

W kilku miejscach tego poradnika znajdują się dobre rady, których stosowanie może skutecznie zmniejszyć ryzyko padnięcia ofiarą ataku phishingowego, czy ransomware'owego. Kilkakrotnie jednak w tym poradniku jest wzmianka o różnego rodzaju kontach, ich przejęciu i wyciekach danych. Podstawowym zabezpieczeniem konta w jakimkolwiek serwisie jest obecnie hasło. I choć to wydaje się trywialne, ostatnie wydarzenia, chociażby na scenie politycznej i utrata kontroli nad kontami twitterowymi polityków, pokazują, że wiedza na temat tworzenia bezpiecznych haseł, ich przechowywania oraz dwuskładnikowej weryfikacji, wcale nie jest taka powszechna, jak być powinna. Jednym z głównych grzeszków internautów jest używanie jednego hasła do wszystkich lub wielu serwisów internetowych. To prosta droga do przejęcia konta przez atakującego. Po lekturze wcześniejszych rozdziałów tego poradnika nie jest chyba dla nikogo zaskoczeniem, że potężne bazy danych loginów, adresów mail i haseł wypływają co jakiś czas i nawet najwięksi mieli już z tym problem, wymienić można by chociażby Facebooka, Dropboxa, LinkedIn i inne. Używając jednego hasła do wielu serwisów narażamy się na przejęcie wielu

swoich kont jednocześnie. Jeśli więc wyciekła baza danych użytkowników LinkedIn, a to samo hasło mamy do Facebooka i jeszcze kilku innych, to nie są to już nasze konta.

Na skróty: Kto może kserować nasz dowód osobisty? Podmioty, które mają prawo w toku świadczonych przez siebie usług kserować dowód osobisty klienta wymienione są w Ustawie z dnia 1 marca 2018 roku o Przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. Dokumentów klienta nie mają prawa kserować np. siłownie. To prosta droga do utraty tożsamości. Jeśli już musisz wykonać skan swojego dokumentu tożsamości zasłoń te dane, które nie są konieczne do weryfikacji jakiejś usługi. Możesz także dodać na skanie znak wodny z datą i wpisanym konkretnym celem dla którego został on wykonany.

Drugim problemem, od wielu lat, pozostaje to, jakich haseł używamy. Stosujemy hasła łatwe do zapamiętania, bardzo proste ze względu na swoją konstrukcję, zawierające istniejące w słowniku wyrazy. Stosujemy również hasła, które ktoś, kto zdobył dostatecznie dużo informacji na nasz temat, może po prostu zgadnąć. Takim sposobem doszło do włamania na twitterowe konto byłego już prezydenta Donalda Trumpa. Na dodatek, nie dość, że stosujemy hasła bardzo łatwe do złamania (np. za pomocą ataku słownikowego), to jeszcze zapisujemy je w bardzo widocznych miejscach.

W 2011 roku kamera Szkła Kontaktowego nagrała laptopa z którego korzystał ówczesny premier, Donald Tusk. W widocznym miejscu miał on zapisany login oraz hasło.

Jak więc się zabezpieczać? Podstawowe zasady bezpieczeństwa mówią o stosowaniu haseł, co najmniej, ośmioznakowych, złożonych z dużych i małych liter, cyfr i znaków specjalnych. Nie należy stosować haseł, które stanowią wyrazy ze słownika lub które mogą w jakikolwiek sposób kojarzyć się z nami (np. imienia psa czy kota). Nie należy również, jak już zostało wspomniane, stosować jednego hasła to kilku usług. Idealnym rozwiązaniem jest zastosowanie menedżera haseł. To specjalna, szyfrowana aplikacja, która generuje oraz zapamiętuje długie, skomplikowane i niepowtarzalne hasła. Można go także skonfigurować tak, aby był połączony z przeglądarką internetową i automatycznie uzupełniał pole hasła. W ten sposób, jako użytkownik, nie musimy znać żadnych haseł, poza tym, które daje nam dostęp do samego menedżera.

Błędem z perspektywy czasu okazała się również polityka dotycząca zmiany haseł, co jakiś określony czas (np. wymuszanie przez administratora systemu zmiany hasła co 30 dni). Takie przymuszanie prowadzi

paradoksalnie do obniżenia bezpieczeństwa generując niebezpieczne patologie w tym zakresie. Użytkownik zmuszany do zmiany swojego hasła co 30 dni stosuje najczęściej metodę stałego członu hasła oraz dodaje niego cyfry będące np. aktualnym miesiącem (01, 02, 03, 001, 002, itd.) lub aktualnym rokiem (2020, 2021, itd.). Znacznie bezpieczniej dla systemu jest zatem ustalenie jednego, niepowtarzalnego, odpowiedniego długiego, skomplikowanego, ale niezmiennego hasła, niż tworzenie co miesiąc nowej wariacji tego samego, łatwego do odgadnięcia schematu.

Dwuskładnikowa weryfikacja

Wiele dostępnych serwisów internetowych daje możliwość dodatkowego zabezpieczenia swojego konta poprzez dwuskładnikowe uwierzytelnianie. Polega to na tym, że przy każdej próbie logowania na konto, oprócz standardowego loginu i hasła, użytkownik będzie musiał podać jeszcze wygenerowany, jednorazowy kod, który dostarczony zostanie, według wybranej opcji, na numer telefonu komórkowego lub wygenerowany zostanie w aplikacji uwierzytelniającej zainstalowanej na telefonie (np. *Google Authenticator*). Zapobiegnie to nieuwierzytelnionemu logowaniu, dostęp do końca nie będzie bowiem możliwy bez podania tego kodu. Jedną z metod dodatkowego uwierzytelniania jest również fizyczny klucz U2F.

Klucz Universal 2 Factor to urządzenie przypominające swoim wyglądem pamięć zewnętrzną i tak też się z niego korzysta. Urządzenie to

jest wpinane w port USB komputera. Skonfigurowane na stronie obsługującej takie uwierzytelnianie za pomocą klucza sprzętowego generuje parę kluczy, które tam też (w danym serwisie) są przetrzymywane. Powoduje to, że klucza możemy teoretycznie użyć na nieskończonej ilości serwisów. Po skonfigurowaniu go, przy próbie logowania serwis w którym mamy konto wysyła tzw. challenge, który zostaje podpisany przez nasze urządzenie i wysłany z powrotem. Nasz klucz współpracuje bezpośrednio z przeglądarką co czyni go niepodatnym na ataki typu *keylogger* czy *phishing*.

Klucza sprzętowego można używać w przeróżnych serwisach. Jako przykład niech posłuży nam w tym przypadku Facebook. Uwierzytelnianie dwuskładnikowe skonfigurować można wchodząc w zakładkę *Ustawienia i prywatność*, *Ustawienia* oraz opcję *Bezpieczeństwo i logowanie*. Tam znajduje się opcja *Uwierzytelnianie dwuskładnikowe* i *Klucz zabezpieczeń*. Konfiguracja jest banalna, w pewnym momencie konieczne jest jedynie dotknięcie klucza. Tak samo będzie w momencie, kiedy po skonfigurowaniu będziemy chcieli się w jakimś serwisie zalogować. Nie ma praktycznie możliwości, żeby takie zabezpieczenie obejść. Klucz trzeba mieć jednak przy sobie, niektóre serwisy proponują wydrukowanie i zachowanie w bezpiecznym miejscu kodów ratunkowych, które pozwolą wam odzyskać konto w przypadku uszkodzenia lub zagubienia klucza.

Fake newsy

Internet jest pełen wielu wartościowych rzeczy, mieści się w nim niemal cała wiedza obecnie dostępna ludzkości. Ten sam Internet to jednak również rezerwuarem wszelkiego rodzaju bzdur i teorii spiskowych. Ich popularność potęgowana jest niestety sposobem w jaki działają wyszukiwarki internetowe, które premiują i promują treści nie najbardziej rzetelne, a te najpopularniejsze. A co klika się bardziej, niż obietnica dostępu do jakiegoś skandalu, spisku, czy tajemnicy? W tej drugiej kategorii mieszczą się fake newsy, czyli nieprawdziwe, bądź zmanipulowane informacje, których autorzy mają wiele różnych powodów, żeby zwabić, zmanipulować, a następnie zasiać w tobie ziarnko niepewności. Na tyle duże, żeby skłonić cię do podzielenia się ich głupotami publicznie. I tak koło się zamyka.

Fake newsy to nic nowego

Jednym z większych błędów z jakimi spotykamy się na co dzień opowiadając o fake newsach jest przekonanie, że są one czymś nowym - wymysłem XX i XXI wieku. To nieprawda. Nieprawdziwe informacje były przekazywane, z różnych pobudek, już od zarania dziejów. W XIII wieku p.n.e Ramzes II rozpowiadał o druzgocącym zwycięstwie Egipcjan nad wojskami hetyckimi w bitwie pod Kadesz. Znający historię wiedzą, że w bitwie pod Kadesz sytuacja była nieco bardziej skomplikowana, a Epipcjanom do druzgocącego zwycięstwo brakowało wiele. W trakcie I Wojny Światowej antyniemiecka propaganda brytyjska rozprzestrzeniała nieprawdziwe informacje o istnieniu tzw. Fabryki Zwłok (*Kadaververwertungsanstalt*)

w której ciała poległych żołnierzy przetapiane były na tłuszcz z którego wyrabiano nitroglicerynę, mydło, świece i wosk różnego zastosowania. Istnienie takich fabryk było całkowitą nieprawdą, którą później o ironio, w swojej propagandzie, używał Joseph Goebbels w (skutecznym) negowaniu doniesień o eksterminacji przez hitlerowski reżim ludności pochodzenia żydowskiego. Sama machina propagandowa Goebbelsa i III Rzeszy może sama w sobie być przykładem fabryki nieprawdziwych i zmanipulowanych informacji, produkowanych na potrzeby polityczne. Przykłady tego typu z historii świata można mnożyć.

Dziś, w czasach, kiedy stronę internetową może mieć każdy, a jej założenie trwa kilka minut, pisanie nieprawdy i trafianie z tym do milionów odbiorców jest prostsze, niż kiedykolwiek. Niebagatelny udział mają w tym

procederze serwisy społecznościowe w których nieprawdziwe informacje typu *koronawirus nie istnieje i jest jedynie przykrywką dla wprowadzania 5G, czy Bill Gates jest odpowiedzialny za obecną pandemię, żeby potem zarobić na szczepionkach* (swoją drogą te dwie tezy wykluczają się nawzajem) udostępniane są następnie na tysiącach, a nawet milionach profili i fan page'y.

Na skróty: Po co powstają fake newsy? Z różnych pobudek. Niektóre dla żartu, niektóre dla propagandy, inne są działaniem dezinformacyjnym obcych służb, grup wpływu, czy terrorystów. Są i takie, które mają charakter ekonomiczny i powstają, aby zasiać niepokój w pewnej sprawie, a następnie sprzedać na wygenerowany przez siebie problem odpowiednie lekarstwo, czy produkt.

Jak powstaje fake news?

Recepta na fake newsa jest dość prosta. Czasem są to informacje całkowicie zmyślone, nie poparte żadnymi faktami - jak np. lądowanie kosmitów na biegunie północnym, częściej jednak to dość zmyślne manipulacje wplątujące fakty w całkowicie nieprawdziwe wydarzenia i domysły. Tak było np. ze słynnym już *Event 201* na którym dyskutowano o rozwiązaniach w przypadku wystąpienia światowej pandemii. Aktualna sytuacja na świecie związana z epidemią koronawirusa jest wprost wymarzoną dla wszystkich spiskowców, hipotez pochodzenia wirusa, przebiegu epidemii i szczepień jest tak wiele, że trudno nad nimi wszystkimi nadążyć, a ich sympatykom zupełnie nie przeszkadza, że nauka wykluczyła

już bardzo wiele z przedstawianych przez nich tez. Zobaczmy więc, jak w bardzo łatwy sposób da się spreparować fake newsa.

Pod koniec 2019 roku archeolodzy odkryli w pobliżu starożytnego miasta Teby w Egipcie 20 doskonale zachowanych sarkofagów. Starożytne trumny najprawdopodobniej pochodzą z około 1540 roku przed naszą erą. "To jedno z największych i najważniejszych odkryć archeologicznych w historii", mówili przedstawiciele rządu egipskiego tuż po dokonaniu odkrycia. Był to jednak jedynie początek tego, co miało nadejść. Po otwarciu sarkofagów, dokładnie dwudziestu, jak rok 20 20 (przypadek?) zaczęły dziać się dziwne rzeczy. Uczestniczący w badaniach naukowcy zaczęli umierać jeden po drugim. Badający ich lekarze jako przyczynę zgonu wskazywali niewydolność oddechową.

U każdego. Bezpośrednio przyczynić do zgonów tych ludzi miał się nieznany dotąd wirus. Rząd Egiptu natychmiastowo utajnił sprawę, wysyłając raport jedynie do głów państw największych, światowych mocarstw. Ostatni z uczonych zmarł na początku grudnia ubiegłego roku… w trakcie pobytu w Chinach… w mieście Wuhan. Historia nowego wirusa, a raczej klątwy starożytnych Bogów, którym cywilizacje zachodnie zakłóciły wieczny spoczynek znacie od tej pory już z przekazów mediów. Nie dajcie się ogłupić, otwórzcie oczy i zacznijcie myśleć samodzielnie. Nie dajcie karmić się propagandą z telewizora. Taki wirus nie mógł powstać naturalnie, powyższa historia, o której z pewnością nie słyszeliście w głównych wydaniach serwisów informacyjnych (przypadek?) dobitnie to pokazuje. Chcą to przed Wami ukryć, bo nie wiedzą z czym mają do czynienia. A to dopiero początek klątwy.

Powyższa historia jest prawdziwa do pewnego momentu. W październiku 2019 roku faktycznie odnaleziono 20 doskonale zachowanych sarkofagów w Egipcie (w miejscu w którym wznosiło się starożytne miasto Teby). Naukowcy faktycznie uznali to za jedno z największych odkryć archeologicznych, trumien było faktycznie 20. Cała reszta jest jednak wytworem wyobraźni, aby pokazać czytelnikowi, jakiej manipulacji można dokonać dodając do odrobiny faktów i pewnej koincydencji zdarzeń całą masę bzdur i wyssanych z palca hipotez.

Słabe źródła informacji

Jak więc nie dać nabrać się na manipulacje w sieci? Mówiąc krótko, nie korzystać ze słabych źródeł informacji. A słabe źródła to takie, które cechuje

nieobiektywizm, nacechowanie ideologiczne, odwoływanie się do emocji, jednostronność, krzykliwość i sensacyjność w przekazie, czy nie popieranie się żadnymi tekstami źródłowymi. Należy znać i zdawać sobie także sprawę z tego, jak działa wyszukiwarka internetowa. Fakt, że jakaś strona znajduje się na czele wyszukań nie czyni z niej automatycznie dobrego źródła informacji. Najlepsze źródła informacji, strony naukowe, bardzo często przegrywają ten nierówny wyścig o pozycję w Google już na samym starcie, a to właśnie one są najlepszym możliwym źródłem informacji na jakiś temat.

Autor: Michał Miśko – specjalista d.s. bezpieczeństwa, wykładowca, przewodniczący stowarzyszenia Dobra Informacja, redaktor naczelny portalu Geekweb.pl

Źródła

Społeczeństwo informacyjne w Polsce w 2020 roku, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2020-roku,2,10.html

Rok 2020 w wyszukiwarce Google, https://www.geekweb.pl/internet/item/1562-2020-w-google

W Polsce jest niemal 37 milionów kont internetowych. To prawie tyle, ile całkowita liczba ludności, https://www.geekweb.pl/internet/item/1024-w-polsce-jest-aktywnych-37-milionow-kont-internetowych

Internet Organised Crime Threat Assessment (IOCTA) 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Chcieli zrobić przelew, stracili 940 tysięcy. Ktoś okradł urząd miasta w Jaworznie, https://tvn24.pl/katowice/chcieli-zrobic-przelew-stracili-940-tysiecy-ktos-okradl-urzad-miasta-w-jaworznie-ra507306

Hrabstwo Delaware zapłaciło pół miliona dolarów okupu cyberprzestępcom, https://www.geekweb.pl/inne/wydarzenia/item/1531-hrabstwo-delaware-okup-ransomware

Atak ransomware mógł przyczynić się do śmierci kobiety w Niemczech, https://www.geekweb.pl/inne/wydarzenia/item/1360-atak-ransomware-smierc-kobiety-niemcy

Garmin 'paid multi-million dollar ransom to criminals using Arete IR', say sources, https://news.sky.com/story/garmin-paid-multi-million-dollar-ransom-to-criminals-using-arete-ir-say-sources-12041468

Polska spółka zbrojeniowa ofiarą phishingu. 4 mln zł strat, https://www.bankier.pl/wiadomosc/Polska-spolka-zbrojeniowa-ofiara-phishingu-4-mln-zl-strat-4201570.html

Podawał się za Willa Smitha. Wyłudził od kobiety 45 tys. złotych, https://www.polsatnews.pl/wiadomosc/2020-11-30/podawal-sie-za-willa-smitha-wyludzil-od-kobiety-45-tys-zlotych/

2,8 miliona złotych kary od UODO dla Morele.net, https://www.geekweb.pl/internet/item/809-morele-net-kara-uodo-3-miliony-zlotych

Jak chronić swoje dane osobowe?, https://www.geekweb.pl/software/poradniki/item/835-ochrona-danych-osobowych-pesel

Uważaj na fałszywe sklepy internetowe. NC Cyber wydało ostrzeżenie, https://www.geekweb.pl/internet/item/564-uwazaj-na-falszywe-sklepy-internetowe-nc-cyber-wydalo-ostrzezenie

Fałszywe sklepy wciąż zbierają żniwo, https://www.geekweb.pl/internet/item/744-falszywe-sklepy-wciaz-zbieraja-zniwo

Co to jest chargeback?, https://www.dziennikprawny.pl/pl/a/co-to-jest-chargeback

77,000 Steam users are hacked every month. Here's how Valve is fixing it, https://thenextweb.com/insider/2015/12/10/77000-steam-users-are-hacked-every-month-heres-how-valve-is-fixing-it/

11-latka wydała ponad 22 tysiące złotych na płatności w grze. Ojciec jest w szoku, https://techgame.pl/roblox-070720-sj-11-letnia-dziewczynka-nabila-ogromny-rachunek-w-grze

Google Confirms 'Malicious' Security Threats Hiding On Play Store: Delete These 12 Apps Now, https://www.forbes.com/sites/zakdoffman/2020/02/21/google-confirms-malicious-security-threats-hiding-on-android-play-store-delete-these-12-apps-now/?sh=775edce29fc2

O co chodzi z tymi certyfikatami SSL?, https://www.geekweb.pl/software/poradniki/item/934-certyfikat-ssl

Zdjęcia skąpo ubranej kobiety na profilu posła Suskiego. "To włamanie, nie znam tej pani", https://tvn24.pl/polska/twitter-marek-suski-padl-ofiara-hackerow-zdjecia-rozebranej-kobiety-4942128

Twitter Trumpa został przejęty, twierdzi holenderski portal, https://www.geekweb.pl/inne/wydarzenia/item/1449-twitter-trump-zhakowany

Hasło premiera Donalda Tuska, https://niebezpiecznik.pl/post/haslo-premiera-donalda-tuska/

Jak powstaje fake news?, https://www.geekweb.pl/magazyn-dobrych-tresci/item/946-jak-powstaje-fake-news

2021

O stowarzyszeniu Dobra Informacja

Stowarzyszenie oficjalnie powstało 28 września 2020 roku. Działa na polu propagowania wiedzy naukowej - wiele w tej kwestii jest do zrobienia - edukacji w zakresie bezpieczeństwa w sieci, przeciwdziałania dezinformacji oraz edukacji i promocji nowych technologii. Misją stowarzyszenia jest również wskazywanie wartościowych źródeł informacji, a także identyfikacja i edukacja w zakresie fałszywych lub zmanipulowanych informacji. Stowarzyszenie jest również wydawcą portalu internetowego Geekweb.pl.

Nie każda informacja musi być dobra, ale każda powinna być, pełna, obiektywna i rzetelna.

Kontakt: czesc@dobrainformacja.edu.pl