sieć na kulturę

BEZPIECZNE ZACHOWANIA W SIECI

PODRĘCZNIK

Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
FWZR
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Wprowadzenie

DWA ŚWIATY?

Żyjemy w świecie, w którym liczba urządzeń podłączonych do sieci jest większa niż liczba ludzi żyjących na planecie Ziemia. Prawie każdy z nas ma swój komputer, a niekiedy także dodatkowo smartfon czy tablet. Nie zapominajmy też o różnych konsolach do gier (także sieciowych), czy inteligentnych telewizorach, lodówkach, samochodach, pralkach, a nawet żarówkach. Jakby na to nie patrzeć, to także swego rodzaju komputery lub urządzenia bezpośrednio z nimi połączone. W związku z tym wszyscy nieustannie jesteśmy zagrożeni, a rzadko kiedy zdajemy sobie sprawę z liczby i źródeł niebezpieczeństw. Nie można dać się ponieść emocjom i na każdym kroku wypatrywać przestępstw i wykroczeń, ale i nie można także całkowicie uśpić swoją czujność. Zasada zdrowego rozsądku, tak jak zazwyczaj sprawdza się w realnym świecie, ma szansę zadziałać także i w wirtualnej rzeczywistości.

Szacuje się, że od 2013 roku codziennie wykradanych jest prawie 4 miliony rekordów. Oznacza to, że co sekundę wykradane jest przynajmniej kilkadziesiąt danych. Codziennie pojawia się też kilkaset tysięcy nowych próbek złośliwego oprogramowania. Przy tak dużej liczebności cyfrowych przestępstw, możliwość, że dotkną one także i nas jest naprawdę olbrzymia.

Różnego typu internetowe przestępstwa przekładają się na nasze realne życie. Przez działania cyberprzestępców mogą zginąć pieniądze z konta, dane, którymi posługujemy się w realnym świecie, mogą zostać wykorzystane do przestępstw, a nasze prywatne zdjęcia stać się obiektem żartów i kpin, które dla nas wcale nie będą ani zabawne, ani przyjemne.

PO CO NAM WIEDZA O BEZPIECZEŃSTWIE W INTERNECIE?

Dlatego tak ważne jest, aby rozumieć, jak działają cyberprzestępcy, jakie są ich cele i metody oraz starać się nie narażać niepotrzebnie na wszelkie zagrożenia. Jeżeli jesteśmy podłączeni do Internetu, to absolutnie wszyscy jesteśmy narażeni na ataki. Tak naprawdę

nikt nie jest bezpieczny w stu procentach. Możemy jednak wykonać wiele działań, które wzmocnią nieco nasze bezpieczeństwo, a tym samym cyberprzestępcom będzie trudniej nas zaatakować.

Warto pamiętać, że na tym etapie kultury cyfrowej, na jakim właśnie się znajdujemy, nie ma możliwości całkowitego zabezpieczenia się przed różnymi, niechcianymi działaniami cyberprzestępców. Od jakiegoś czasu zapobieganiu i ściganiu cyberprzestępstw zajmują się specjalne wydziały policji. Ich działania także nie są w stanie całkowicie zniwelować różnych zagrożeń. Dokładnie jak w realnym świecie. Pomimo policyjnych kontroli radarowych nie mamy pewności, że jakiś kierowca wbrew przepisom i zdrowemu rozsądkowi nie spowoduje zagrożenia dla innych, jadąc po mieście z zawrotną prędkością.

Dlatego tak ważne jest wytworzenie u siebie zespołu zachowań, które pozwolą nam zorientować się, że mamy do czynienia z cyfrowym niebezpieczeństwem. Pomimo istnienia dobrze rozbudowanej infrastruktury oprogramowania antywirusowego, systemów bezpieczeństwa oraz kontroli, lub jak kto woli cenzury, Internetu, to wciąż użytkownik sieci — jego zachowania i nawyki — stanowią najsłabszy punkt w procedurach bezpieczeństwa, w który najłatwiej mogą uderzyć przestępcy.

Czy to co napisane powyżej jest prawdą? Warto samemu odpowiedzieć sobie na to pytanie. Udowodnić to może pewien eksperyment skłaniający do autorefleksji. Kto z Was wie, że po skorzystaniu z portalu społecznościowego na swoim smartfonie należy wylogować się z niego w celach bezpieczeństwa? Okey. A kto ma aplikację społecznościową aktywną całą dobę? Tylko tyle i aż tyle.

Gdzie szukać informacji związanych z bezpieczeństwem w sieci

PROBLEMY Z WYCIEKIEM DANYCH Z SERWISÓW

Nasze dane stały się bardzo cennym towarem na rynku cyberprzestępczym. Dostęp do wiedzy na temat naszych loginów, haseł, ale także informacji o naszych znajomych, planach, wydatkach, hobby jest dziś dość wartościowy. Może nie w przeliczeniu na pieniądze, gdyż na czarnym rynku za komplet informacji o użytkowniku sieci wyceniony został on na mniej niż

1$. Teraz wyobraźcie sobie, że w pakiecie kilkuset osób, których dane zostały wykradzione, jesteście także i Wy. Co może zrobić z takimi danymi cyberprzestępca? Możliwości jest wiele: wziąć na Wasze konto kredyt, wyłudzić odszkodowanie od firmy ubezpieczeniowej, wyrobić dokument, który następnie wykorzysta w niecnych celach… Resztę pozostawmy wyobraźni.

Nie jest już też tajemnicą, że wielkie firmy płacą za dostęp do tych informacji, by np. lepiej tworzyć reklamy produktów w taki sposób, aby odpowiadały naszym zainteresowaniom i potrzebom. Jeżeli ktoś interesuje się samochodami, prawdopodobnie otrzyma reklamy związane z motoryzacją, a nie np. z nowinkami modowymi. Jednak tzw. profilowana reklama, choć zazwyczaj niechciana i zbyt nachalna, to najmniejszy problem, z jakim przyjdzie nam się zmierzyć, gdy ktoś dowie się o nas zbyt wiele…

Zakupem takich informacji zainteresowani są także tzw. brokerzy danych. Skupują oni informacje o ludziach, aby później sprzedać je np. firmom ubezpieczeniowym, agencjom HR, agencjom reklamowym, agencjom odpowiedzialnym za kampanie polityczne. Chętnych na zakup tych danych jest naprawdę wielu, choć mało który z nich chciałby się ujawnić. Co z tego może wynikać? Wyciek danych może się odbić na przyszłości użytkowników sieci. Interesujesz się sportami motorowymi — zapłacisz większe ubezpieczenie za samochód (pewnie też jeździsz jak rajdowcy). Zbyt wiele czasu spędzasz na grach komputerowych — możesz nie dostać pracy (jak ktoś uzna, że interesujesz się tylko zabawą). Każda dana mówi coś o nas, a możliwości ich wykorzystania jest wiele.

KONSEKWENCJE

Kiedy z jakiegoś portalu lub innego miejsca w sieci, które wymaga logowania, wycieką nasze dane, konsekwencje mogą nas nieprzyjemnie zaskoczyć. Cyberprzestępcy dysponują oprogramowaniem, które automatycznie sprawdzi, czy wykradzione dane do logowania, np. do poczty internetowej, nie są takie same jak do konta bankowego, portalu społecznościowego, platformy do gier, itp. Jeżeli zaś posługujemy się wszędzie tym samym loginem i hasłem, mają możliwość przejęcia naszych kont z różnymi usługami i funkcjami. Łatwo zaś wyobrazić sobie, co mogą zrobić, znając login i hasło np. do banku czy serwisu społecznościowego.

CO MOŻEMY ZROBIĆ, ABY CZUĆ SIĘ BEZPIECZNIEJ?

Mogłoby się wydawać, że zabezpieczenie naszych danych w różnych internetowych serwisach to nie nasz problem. W końcu podając je podczas rejestracji do jakiejś usługi, zaufaliśmy jej dostawcy, który zobowiązał się chronić nasze dane jak najlepiej. Ale… wpadki

zdarzają się najlepszym. Wycieki danych dotknęły tak duże i szanowane serwisy jak Twitter, eBay, Canva, a to tylko kilka najbardziej znanych przypadków. Pamiętajmy także i o tych, które nigdy z różnych powodów nie zostały ujawnione.

Pojawia się pytanie, co my sami możemy zrobić, aby czuć się trochę bardziej bezpiecznie:

- Po pierwsze (i najważniejsze), nie powinno używać się tego samego loginu i hasła do wielu usług i serwisów. Być może dobrym rozwiązaniem jest wykupienie usługi 1password (1password.com), umożliwiającej tworzenie i zapamiętywanie skomplikowanych haseł do wielu serwisów, przy konieczności zapamiętania jedynie jednego. Jednakże jest to usługa płatna i nie każdy może sobie na nią pozwolić.
- Po drugie, myśleć o tym, komu i w jakim celu udostępniamy nasze dane. Nie każdy serwis musi wiedzieć o nas wszystko. Już w momencie podawania rozmaitych danych w procesie rejestracji niekiedy powinno zapalić się nam w głowie czerwone światło ostrzegawcze.
- Po trzecie, jeżeli mamy taką możliwość, zawsze powinniśmy korzystać z uwierzytelniania dwuetapowego (np. potwierdzenie logowania kodem SMS, odciskiem palca czy korzystać z systemu rozpoznawania twarzy).

Ćwiczenie:

Aby sprawdzić, z jakich serwisów wykradziony został nasz adres e-mail (oraz inne dane), warto skorzystać ze strony: **haveibeenpwned.com**. Nie załamujcie rąk, jak dowiecie się, że z jakiegoś serwisu wyciekł Wasz adres. Na dobry początek zmieńcie hasła do logowania w tym serwisie lub usłudze i wszystkich innych, które są z nimi związane.

Warto też zaglądać (najlepiej regularnie) na stronę **Niebezpiecznik.pl**. To jeden z najstarszych i najbardziej profesjonalnych serwisów zajmujących się cyfrowym bezpieczeństwem.

Narzędzia niezbędne do wykonania ćwiczenia:

Komputer z dostępem do Internetu, przeglądarka internetowa np. Mozzilla Firefox, Chrome, Internet Explorer etc.

Przeczytacie w nim między innymi o różnych wyciekach danych z serwisów, jakie w ostatnim czasie zostały ujawnione. Pomimo, że osoby prowadzące Niebezpiecznik skomercjalizowały swoje działania, skupiając się przede wszystkim na szkoleniach dla firm, wciąż informacje publikowane na ich blogu są wiarygodne, aktualne, a przede wszystkim napisane językiem

zrozumiałym dla przeciętnego użytkownika Internetu. Do ciekawych działów prowadzonych na stronie należą: *CSI Stories* w humorystyczny sposób przedstawiające przygody hakera Janusza oraz podcast *Na podsłuchu*, w którym redaktorzy serwisu rozmawiają o różnych zagrożeniach pojawiających się w wirtualnej przestrzeni. Zasadne jest też zaglądanie do *Memdump*, czyli zestawienia skrótowych informacji na temat różnych niebezpiecznych cyfrowych zjawisk, których ze względu na brak czasu i liczbę zagrożeń nie udało się szerzej opisać. Na zachętę warto wysłuchać wykładu wygłoszonego przez Piotra Koniecznego (założyciela serwisu Niebezpiecznik.pl) pt. *3 mity cybersecurity* na konferencji TEDxKatowice.

Konferencje firmowane marką TED (Technology, Entertainment and Design) *nastawione są na* promowanie idei wartych propagowania. Dlatego temat bezpieczeństwa cyfrowego pojawia się na nich dość często. Warto w wolnej chwili posłuchać, co na temat wycieku danych z sieci (i innych związanych z bezpieczeństwem cyfrowym) mają do powiedzenia specjaliści.

Innym godnym polecenia miejscem w sieci, gdzie szeroko opisywane są wycieki danych z serwisów internetowych, jest blog Kaspersky Daily: **plblog.kaspersky.com**. Blog znanego producenta oprogramowania antywirusowego udostępnia (w języku polskim) i przejrzyście omawia problemy interesujące nas w tym rozdziale.

Ciekawy blog prowadzony przez firmę specjalizującą się w cyberbezpieczeństwie i oprogramowaniu antywirusowym to także: **blog.avast.com**.

Lubicie kryminały, a macie ukończone 16 lat? Świetnie. Na rynku wydawniczym pojawiła się ciekawe powieści autorstwa Jakuba Szamałka pt. *Cokolwiek wybierzesz* i *Kimkolwiek jesteś* składające się na cykl *Ukryta sieć*. Dzięki nim, uczestnicząc w dziennikarskim śledztwie bohaterki książek, będziecie mieli okazję zapoznać się ze wszystkimi informacjami, jakie znajdziecie w tym rozdziale, a nawet w całym podręczniku. Pod względem merytorycznym autor wie, co opisuje.

W ostatnim czasie Google wprowadziło usługę sprawdzenia, czy problem wycieku haseł z różnych serwisów i usług w sieci dotknął już także i Was. Przy okazji dowiecie się, jak silne hasła stosujecie i które z nich powtarzają się w różnych usługach. Uwaga! Usługa dotyczy tylko haseł zapisanych w przeglądarce Chrome.

Ćwiczenie:

Zapoznajcie się z różnymi wpisami z bloga *ptr na **niebezpiecznik.pl**. W zespołach opowiedzcie sobie o wpisie, który zwrócił Waszą uwagę Wybierzcie Waszym zdaniem najciekawszą historię i przedstawcie ją na forum w lekkiej, najlepiej humorystycznej i anegdotycznej formie charakterystycznej dla stand-up'ów.

Narzędzia niezbędne do wykonania ćwiczenia:
Komputer z dostępem do internetu, przeglądarka internetowa np. Mozzilla Firefox, Chrome, Internet Explorer etc.

Gdzie szukać informacji związanych z bezpieczeństwem w sieci

OSZUSTWA

Jest bardzo wiele typów oszustw internetowych. Jedne są mniej, inne bardziej niebezpieczne. Nie sposób nauczyć się wszystkich, choćby dlatego, że w momencie, gdy piszemy ten tekst, powstało przynajmniej kilka nowych sposobów oszukiwania obywateli cyfrowego świata. O nowych formach oszustw internetowych słyszy się każdego dnia. Pewnie każdy zna przynajmniej jedną ofiarę, która przez brak wiedzy, łatwowierność, naiwność lub chwilowo uśpioną czujność dała się podejść cyberprzestępcom.

Niektóre z form cyfrowego oszukiwania zostały przejęte wprost ze świata realnego. Metody „na wnuczka", „na policjanta", „na listonosza", o których kilka lat temu informowała seniorów policja, dziś zostały przeniesione do sieci. Zasady działania są zazwyczaj takie same, a struktura internetu ułatwiająca przestępcom podszywanie się pod różnych ludzi i instytucje sprawia, że oszustów przybywa każdego dnia. Ogólna wiedza w zakresie internetowych oszustw jest dość duża. Ciągle pojawiają się przecież prewencyjne komunikaty medialne. Mimo wszystko wciąż są tacy, którzy z łatwością stają się ofiarami. Tracą pieniądze, swoje dane lub dobre imię.

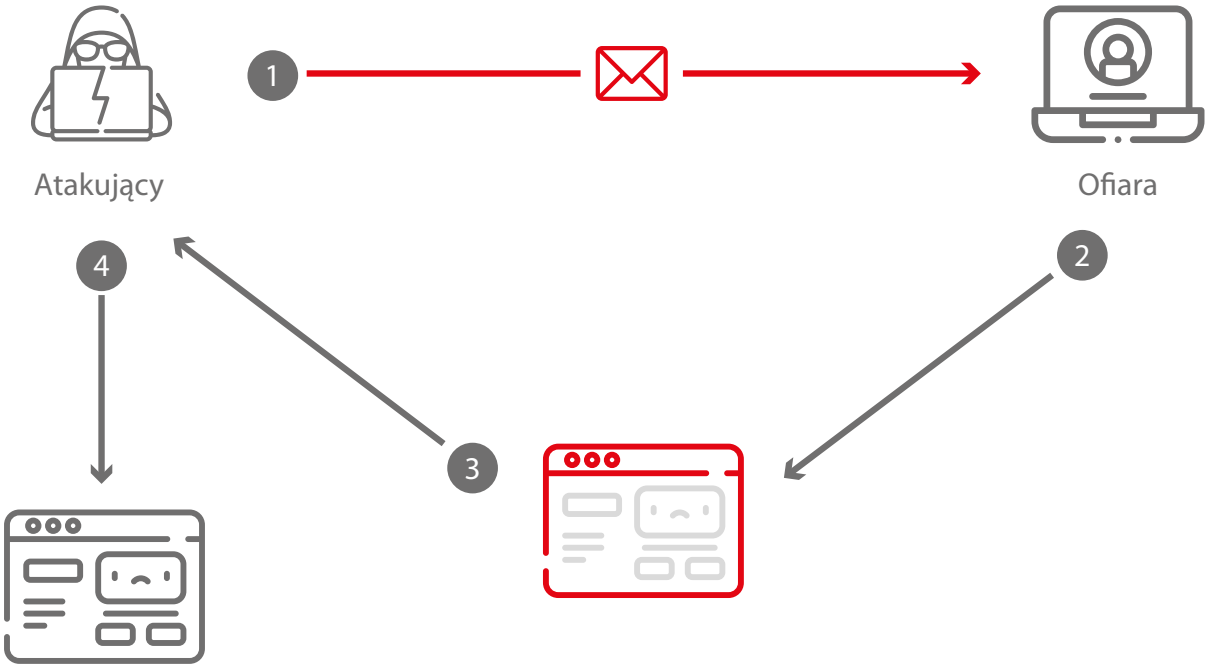
W tym rozdziale skupimy się na kilku, bardzo popularnych, rodzajach oszustw. Wszystkie z nich związane są z podszywaniem się pod osobę lub instytucję, a celem ich jest wyrządzenie materialnej bądź moralnej szkody nieuważnej bądź nieświadomej ofierze.

PHISHING

Najbardziej rozpowszechniona forma oszustwa cyfrowego to phishing. Kojarzy Wam się z wędkarstwem? I bardzo dobrze. To właśnie łowienie naiwnych bądź nieświadomych zagrożenia obywateli cyfrowego świata na haczyk zarzucony przez cyberprzestępców. Pomysłowość przestępców w zakresie „nielegalnego wędkarstwa cyfrowego" wciąż wzrasta, jednak niekiedy wystarczy znać podstawowe mechanizmy oszustwa, aby się przed nim uchronić.

Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.

Oto schemat działania cyberprzestępcy:



1. Przestępca wysyła ofierze informację z linkiem, który ma zostać otwarty. Może to być rzekomy list z banku, w którym mamy konto, albo dokumenty od jakiejś państwowej instytucji. Innym razem wiadomość od szefa z ważnymi danymi lub powiadomienie z jakiegoś serwisu (np. społecznościowego lub rozrywkowego). Może to także być np. informacja o wygranej na loterii… Trzymajmy się tu przykładu banku.
2. W e-mailu lub niekiedy w wiadomości MMS, wyraźnie jest napisane, aby otworzyć link i wykonać jakieś działanie, np. zalogować się do banku.

3. Kiedy ofiara cyberprzestępstwa otworzy link, pojawi się strona bardzo podobna do strony prawdziwego banku lub instytucji. Ofiara wtedy loguje się prawdziwym loginem i hasłem, ale nie wie, że te dane są przechwytywane przez cyberprzestępcę, ponieważ nie jest to strona autentyczna.

4. Dalej już nic nie stoi na przeszkodzie, aby cyberprzestępca zalogował się, używając naszych prawdziwych danych, do banku i … ukradł nam pieniądze.

Bardzo często w tego typu przestępstwach wykorzystywana jest wiedza psychologiczna. Można nawet powiedzieć, że współczesny cyberoszust to bardziej psycholog lub socjolog niż informatyk. Musi wiedzieć, jakie nawyki ma jego ofiara lub grupa ofiar, na którą zastawiana jest pułapka. Niekiedy, gdy planowane jest oszustwo na dużą skalę, zostaje ono poprzedzone długotrwałymi badaniami społecznymi lub obserwacjami potencjalnej ofiary.

Ofiara najczęściej jest nakłaniana do szybkiego działania przez wzbudzanie silnych emocji, np. strachu (np. konto w Twoim banku zostało zablokowane) lub euforii (np. nagroda w konkursie). Kiedy w grę wchodzą emocje, osłabione zostaje racjonalne myślenie. Bo jak tu nie kliknąć, gdy właśnie dowiedzieliście się, że wygraliście najnowszy model smartfona, o którym marzyliście od kilku tygodni? Zasada jest dość prosta. Prawdopodobieństwo, że ktoś współcześnie da Wam coś za darmo, jest znikoma. Cuda rzadko się zdarzają, więc nie ma co ulegać nierealnym obietnicom.

Dlatego tak ważne jest, aby nigdy nie otwierać linków, które wydają nam się podejrzane. Jeżeli mamy jakieś wątpliwości, należy zawsze logować się z poziomu konkretnych stron internetowych, wpisując w pole adresu nazwę strony.

SPEAR FISHING

To cyberpolowanie z harpunem na wybraną osobą. O ile w przypadku phishingu zarzucana najczęściej jest sieć, z nadzieją, że złapią się na nią jakieś ofiary, tak w przypadku spear phishingu cyberprzestępca poluje na jedną, konkretną ofiarę. Proces ataku poprzedzony jest zebraniem informacji o ofierze. Dokonywana jest często jej analiza psychologiczna, a codzienne zachowania cyfrowe i nawyki są dokładnie analizowane. Po zebraniu kompletu informacji przestępcy zastawiają spersonalizowaną pułapkę. Najpopularniejszą ofiarą spear phishingu w ostatnich latach była Hillary Clinton. Ataku dokonano w czasie jej kampanii prezydenckiej.

WHALING

Whaling, czyli wielorybnictwo, to polowanie przestępców na tzw. grube ryby - właścicieli olbrzymich firm lub osoby pełniące w nich kierownicze stanowiska. Wiadomości phishingowe mające wyłudzić różne informacje lub zmusić do konkretnego działania są personalizowane i formułowane w taki sposób, jakby pochodziły od wspólników, zwierzchników lub współpracowników. Typowa wiadomość ma wyglądać jak korespondencja służbowa oraz zawierać jak najwięcej szczegółów wskazujących na jej prawdziwość.

CLONE PHISHING

Oszustwo polegające na dodawaniu do autentycznych maili zainfekowanych załączników. Często jest tak, że w clone phishingu działa mechanizm samonapędzający. Zainfekowany email, otwarty na komputerze nieświadomego użytkownika, automatycznie rozsyła się do wszystkich osób, które posiada on w swojej książce adresowej.

PHARMING

To forma phishingu dość trudna do zweryfikowania przez zwykłego użytkownika Internetu. Po wpisaniu prawidłowego adresu www (np. banku) internauta zostaje przekierowany na fałszywą, ale wyglądającą identycznie (lub niemal identycznie) stronę phishingową. Próbując zalogować się na niej swoimi prawdziwymi danymi, tak naprawdę udostępniamy je przestępcy, który wykorzysta je do logowania na oficjalnej stronie instytucji. Atak ten wymaga od przestępców dość dużej wiedzy informatycznej.

SCAM

Jest takie powiedzenie, że emocje nie są najlepszym doradcą. Emocje tłumią racjonalne myślenie. Ten jakże ludzki mechanizm funkcjonowania z powodzeniem wykorzystują także i cyberprzestępcy. Pod wpływem silnego stresu podejmujemy zazwyczaj niezbyt trafne decyzje. Podobnie jest z euforią. Gdy pojawia się wizja szczęścia na wyciągnięcie ręki, myślenie schodzi na drugi plan. Większość ludzi zrobi wszystko, aby po to szczęście sięgnąć. Bez względu na koszty i konsekwencje. Refleksja najczęściej przychodzi dopiero po czasie. Niestety zazwyczaj jest już zbyt późno, aby naprawić szkody.

Scam – oszustwo polegające na wzbudzeniu u kogoś zaufania, a następnie wykorzystanie tego zaufania do wyłudzenia pieniędzy lub innych składników majątku. Osoba wzbudzająca

fałszywe zaufanie zwykle działa na jedną z ludzkich cech charakteru, zarówno negatywnych, jak i pozytywnych, takich jak: pycha i chciwość, ale też empatia i altruizm.

Źródło: pl.wikipedia.org/wiki/Scam

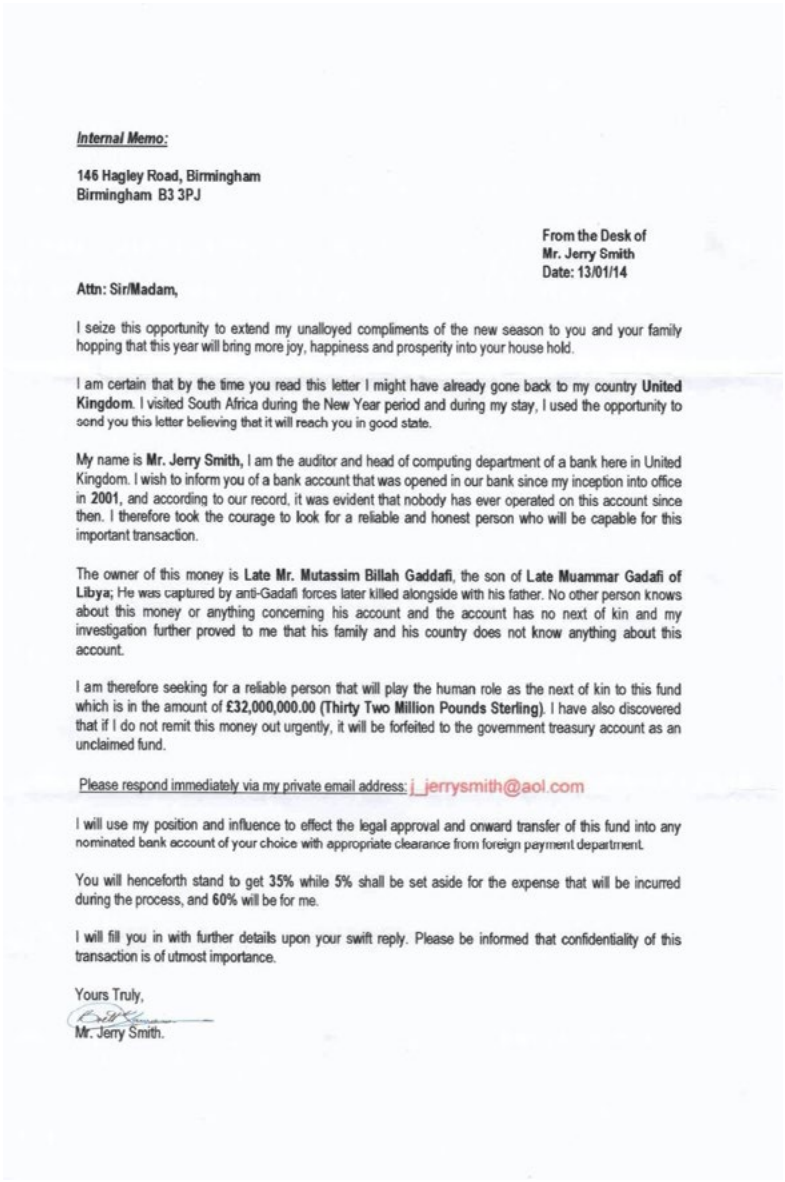
Scam różni się od phishingu tym, że cyberprzestępca musi wzbudzić nasze zaufanie. Jedną z najbardziej popularnych form scamu jest historia z otrzymanym przez kogoś spadkiem. Ofiara cyberprzestepstwa otrzymuje e-mail, z którego dowiaduje się, że dostanie sporą sumę pieniędzy za np. pomoc w opłaceniu adwokata. Ofiara proszona jest więc o wpłacenie drobnej kwoty na jakieś konto. Oczywiście nigdy żadnego spadku nie otrzyma. W takich wysyłanych ofiarom wiadomościach można także przeczytać historie zwierząt przebywających w schroniskach, czy prośby o wsparcie rodziców, których nie stać na leczenie ciężko chorego dziecka. Oczywiście cyberprzestępca poprosi o jakąś sumę pieniędzy, często dołączając fałszywe zdjęcia czy dokumenty medyczne. Ta forma wyłudzeń jest wyjątkowo szkodliwa społecznie z tego względu, że zabija naszą empatię i chęć altruistycznej pomocy.

Pamiętaj, że dziś istnieje wiele portali, które zajmują się legalną zbiórką pieniędzy na różne cele. Robią to zgodnie z prawem i opisują prawdziwe historie. Jeżeli masz potrzebę, by kogoś wesprzeć finansowo, skorzystaj z nich.

Nigdy nie wierz, że ktoś obcy chce podarować Ci olbrzymie pieniądze za drobną usługę. Takie sytuacje zdarzają się jedynie w baśniach, a i tam nie zawsze kończą się happy endem.

NIGERYJSKI SZWINDEL

Jednym z najpopularniejszych oszustw, na które nabrali się ludzie na całym świecie, jest tzw. Nigeryjski szwindel. W swych różnych wersjach autor listu informował ofiary tego rodzaju phishingu o otrzymaniu olbrzymiego spadku od dalekiego krewnego z odległej Afryki. W innej wersji ofiary miały pośredniczyć w różnych operacjach finansowych, ponieważ prawowity dziedzic afrykańskiej fortuny chciał uniknąć podatków, ubezpieczeń lub innych mechanizmów prawno-skarbowych. Pierwsze tego typu listy pojawiły się już w latach 70; a wraz z rozwojem internetu stały się plagą. Gdy mechanizm działania przestępcy nie był jeszcze dobrze znany, dzięki listom z Afryki w latach 90. udało się wyłudzić od użytkowników sieci 100 milionów dolarów.



Internal Memo:

146 Hagley Road, Birmingham
Birmingham B3 3PJ

From the Desk of
Mr. Jerry Smith
Date: 13/01/14

Attn: Sir/Madam,

I seize this opportunity to extend my unalloyed compliments of the new season to you and your family hopping that this year will bring more joy, happiness and prosperity into your house hold.

I am certain that by the time you read this letter I might have already gone back to my country **United Kingdom**. I visited South Africa during the New Year period and during my stay, I used the opportunity to send you this letter believing that it will reach you in good state.

My name is **Mr. Jerry Smith,** I am the auditor and head of computing department of a bank here in United Kingdom. I wish to inform you of a bank account that was opened in our bank since my inception into office in **2001**, and according to our record, it was evident that nobody has ever operated on this account since then. I therefore took the courage to look for a reliable and honest person who will be capable for this important transaction.

The owner of this money is **Late Mr. Mutassim Billah Gaddafi**, the son of **Late Muammar Gadafi of Libya;** He was captured by anti-Gadafi forces later killed alongside with his father. No other person knows about this money or anything concerning his account and the account has no next of kin and my investigation further proved to me that his family and his country does not know anything about this account.

I am therefore seeking for a reliable person that will play the human role as the next of kin to this fund which is in the amount of **£32,000,000.00 (Thirty Two Million Pounds Sterling)**. I have also discovered that if I do not remit this money out urgently, it will be forfeited to the government treasury account as an unclaimed fund.

Please respond immediately via my private email address: j_jerrysmith@aol.com

I will use my position and influence to effect the legal approval and onward transfer of this fund into any nominated bank account of your choice with appropriate clearance from foreign payment department.

You will henceforth stand to get **35%** while **5%** shall be set aside for the expense that will be incurred during the process, and **60%** will be for me.

I will fill you in with further details upon your swift reply. Please be informed that confidentiality of this transaction is of utmost importance.

Yours Truly,
Mr. Jerry Smith.

by HelenOnline, CC BY-SA 3.0, from: Wikimedia Commons.

SMS PHISHING

W latach 70. listy z Afryki dotykały zwykłych obywateli korzystających z tradycyjnej, papierowej poczty. Pamiętajmy jednak, że ta forma oszustwa dokonywana była także za pośrednictwem zwykłej sieci telefonicznej (np. telefony od przestępców podszywających się pod służby specjalne lub agencje rządowe). Wraz z rozwojem komunikacji przeniesiona została także do SMS–ów.

SMS phishing – atak podobny do phishingu polegający na rozsyłaniu SMS-ów, które mają skłonić ofiarę do podjęcia określonego działania.

Źródło: pl.wikipedia.org/wiki/SMS_phishing

Phishing nie tylko dotyczy poczty e-mail, ale również SMS-ów czy wiadomości na komunikatorach. Tym razem zagrożone są smartfony potencjalnych ofiar, na które zastawiona została pułapka. Pamiętać należy o tym, że pod względem użyteczności współczesny telefon to nic innego jak mały komputer. Tam też zainstalowane są aplikacje do obsługi płatności, kont bankowych, poczty internetowej czy, co oczywiste, obsługi SMS-ów i połączeń.

Pamiętaj, że SMS phishing może próbować skłonić Cię do wysłania wiadomości SMS lub oddzwonienia na podany numer telefonu. Często w tym celu wykorzystywane są tzw. SMS PREMIUM lub połączenia PREMIUM. Za ich wysłanie lub wykonanie naliczane są często bardzo wysokie opłaty, które później doliczone zostaną do rachunku telefonicznego.

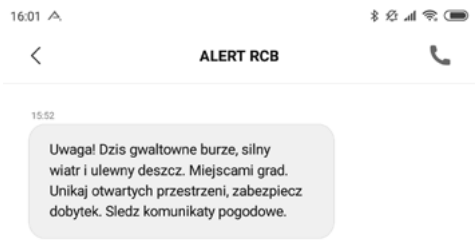
Dobrym adresem, pod którym znajdziecie informacje na temat różnych przestępstw, w tym oszustw internetowych jest: **niebezpiecznik.pl i zaufanatrzeciastrona.pl**

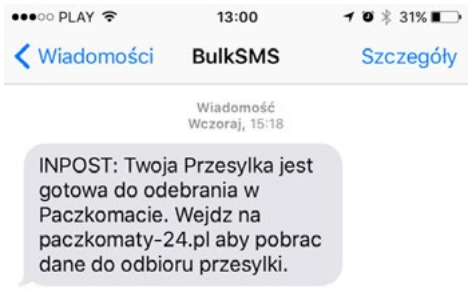
FAŁSZYWA POMOC TECHNICZNA

Jest to forma oszustwa polegająca na nakłonieniu ofiary przez oszusta do zapłacenia za pomoc techniczną. Ofiarami są zazwyczaj osoby posiadające małe kompetencje informatyczne. W tej formie phishingu najczęściej pojawiają się komunikaty o tym, że konto (bankowe, mailowe) zostało przejęte, hasło zostało zmienione, dostęp do internetu może zostać ograniczony itp.

Ćwiczenie:

Przyjrzyj się treści SMS-ów. Jaka jest między nimi różnica?
Który, Twoim zdaniem, jest phishingiem?





SMS phishing rozpoznasz po tym, że ktoś będzie żądał od Ciebie określonych działań. Zwróć uwagę, że w wiadomości ALERT RCB pojawia się wyłącznie informacja o pogodzie. Jeżeli ktoś wysyła do nas SMS i chce, byśmy zalogowali się na jakiejś stronie, powinniśmy uważać to za niebezpieczne.

Ćwiczenie:

Spróbujcie pobawić się w hakerów. Napiszcie mail, SMS i wiadomość na komunikatorze, która będzie miała za zadanie spowodować, że odbiorca-ofiara prześle Wam jakieś dane newralgiczne, np. login i hasło do banku, poczty, itp.

Narzędzia niezbędne do wykonania ćwiczenia:
Komputer z programem do edycji treści lub kartka papieru A4 i coś do pisania: ołówek, długopis.

Ćwiczenie:

Wejdźcie na stronę: **phishingquiz.withgoogle.com** i sprawdźcie swoje umiejętności w rozpoznawaniu phishingu. Uwaga quiz nie jest wcale prosty.

Narzędzia niezbędne do wykonania ćwiczenia:
Komputer z dostępem do internetu, przeglądarka internetowa np. Mozzilla Firefox, Chrome, Internet Explorer etc.

Jak się przed problemami z wyciekiem danych z serwisów oraz oszustwem zabezpieczyć?

Informacje nie są zbyt optymistyczne. Nie można w pełni zabezpieczyć się przed różnymi oszustwami w Internecie oraz cyfrowymi przestępstwami. Podobnie zresztą, jak nie sposób uchronić się przed wypadkami, wykroczeniami czy przestępstwami w realnym świecie.

Nie można jednak załamywać rąk i rezygnować z korzystania z sieci, podobnie jak unikać wychodzenia z domu. W wirtualnej przestrzeni czyhają na użytkowników sieci oszuści i złodzieje, w życiu poza siecią spotkać można na swej drodze złodzieja kieszonkowca lub wpaść pod samochód. Można jednak podjąć różne kroki, które zminimalizują ryzyko bycia oszukanym lub okradzionym. Ważne, aby różne asekuracyjne zachowania związane z rozsądnym zachowaniem w cyfrowym świecie stały się nawykami, które zgodnie ze starym powiedzeniem staną się naszą drugą naturą.

PO CO MI OCHRONA DANYCH, PRZECIEŻ NIE MAM NIC DO UKRYCIA

Przede wszystkim należy obalić mit, że ochrona danych jest niepotrzebna niektórym ludziom, szczególnie jeżeli deklarują, iż prowadzą krystalicznie czysty tryb życia i nic do ukrycia nie mają. Dodatkowo, często argumentują, że są niezamożni, więc nikt nie będzie czyhał na te ich „parę groszy", które mają na koncie. Prawda jest jednak taka, że problem ochrony danych, a co za tym idzie, także i prywatności, to zagadnienie globalne, nad którym nie można przejść obojętnie. Związane jest ono z niezbywalnymi prawami człowieka do ochrony życia i zdrowia swojego, swojej rodziny i bliskich. Odrzucenie przez jednostkę praw do ochrony danych jako „niepotrzebnych" i „zbytecznych" przyczynia się do zgody na inwigilację, podsłuchiwanie, podglądanie innych ludzi. Z ochroną danych i prywatnością jest trochę jak z wolnością słowa. Niektórym nie jest potrzebna, ale nikomu nie powinno się jej ograniczać.

I jeszcze jedno! Nie ma ludzi na świecie, którzy nie mieliby choćby małej tajemnicy, której upublicznienie powodowałoby wstyd lub przynajmniej dyskomfort psychiczny.

Siła ciężkości pytania, czy potrzebna nam ochrona danych, powinna zostać przeniesiona i ograniczona do zagadnienia, jak je zabezpieczyć, aby były one możliwie dobrze chronione.

PLIKI COOKIES

W zasadzie są niezbędne do prawidłowego funkcjonowania stron internetowych. Poprawiają nasz komfort użytkowania różnych portali i serwisów. Informują też nadawców, jakie treści cieszą się większym, a jakie znikomym zainteresowaniem. Zresztą zazwyczaj jesteśmy o nich informowani po wejściu pod konkretny adres w sieci. Nie ma w nich nic złego.

Najczęściej jednym kliknięciem wyrażamy zgody na działanie plików Cookies na jakiejś stronie internetowej. Wszystko jest w porządku do momentu, gdy w gąszczu różnych zgód

związanych z funkcjonowaniem strony, nie pojawiają się i takie, na których wyrażenie wcale nie mamy ochoty. Dotyczą one śledzenia nas na konkretnych stronach, zbierania informacji o naszych zwyczajach (najczęściej konsumenckich) i zachowaniach. Perfidia różnych dostawców treści i usług wykorzystuje nasze lenistwo. Łatwiej jest kliknąć "zaakceptuj wszystkie zgody" niż dokładnie wczytać się, na jaki zakres inwigilacji (śledzenia) im pozwalamy. Na podstawie zebranych danych nadawcy mogą dostosować do nas reklamę, tym samym skłonić nas do zakupów. Mogą również dostosować np. przekaz propagandowy, który będzie próbował nakłonić nas do głosowania na jakiegoś polityka.

Niestety, na podstawie zebranych danych mogą też „nauczyć się" tego, co nas... interesuje. W konsekwencji będą wyświetlać nam w wyszukiwaniach np. tylko te artykuły, które są zbieżne z naszymi poglądami. Przez to damy się zamknąć w tzw. bańce informacyjnej odcinającej nas od informacji ukazujących inny ogląd jakiegoś problemu lub inny punkt widzenia jakiejś sytuacji. To zaś skazuje nas na światopoglądową ślepotę oraz może ograniczać nasz rozwój intelektualny.

Zanim na kolejnej stronie zaakceptujecie jednym kliknięciem wszystkie zgody na działanie „ciasteczek", wczytajcie się dokładnie, czego one dotyczą. Pewnie warto poświęcić kilka sekund więcej i dostosować stosowne zgody do własnych potrzeb i preferencji.

RODO

Ustawa RODO, choć często wyśmiewana i uznawana za „martwą", nieco przyczyniła się do ochrony naszych danych, choćby tych, które udostępniamy na różnych stronach internetowych lub… które analitycy są w stanie wyciągnąć z różnego typu zachowań użytkownika w Internecie.

Unijne przepisy o ochronie danych zapewniają ochronę danych osobowych zawsze, gdy dane te są gromadzone – np. przy zakupach przez internet, ubieganiu się o pracę lub składaniu wniosku o kredyt bankowy. Przepisy te stosuje się zarówno do przedsiębiorstw i organizacji (publicznych i prywatnych) z Unii Europejskiej, jak i spoza niej – takich jak Facebook czy Amazon, które oferują towary i usługi w UE – za każdym razem, gdy takie przedsiębiorstwa i organizacje proszą osoby fizyczne w UE o dane osobowe lub wykorzystują takie dane ponownie.

Format danych nie ma znaczenia – czy to online w systemie komputerowym, czy w dokumencie w formie papierowej – Twoje podstawowe prawa w zakresie ochrony danych muszą być

szanowane za każdym razem, kiedy przechowuje się lub przetwarza dane, które pośrednio lub bezpośrednio identyfikują Cię jako osobę fizyczną.

Źródło: europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_pl.htm

Jeżeli masz jakiekolwiek wątpliwości dotyczące ochrony Twoich danych w sieci, zajrzyj na oficjalną stronę Komisji Europejskiej, gdzie szczegółowo opisane zostały zasady zbierania, przechowywania i przetwarzania danych w internecie:

ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens_pl

DANE WRAŻLIWE

Dane wrażliwe to wszystkie te informacje, które uznajemy za prywatne i nie dzielimy się nimi z obcymi ludźmi. Informacje te podlegają szczególnej ochronie, ponieważ różne firmy czy instytucje nie mogą ich zbierać, udostępniać ani się nimi dzielić.

Oto pełna lista danych wrażliwych:

- dane ujawniające pochodzenie rasowe lub etniczne
- dane ujawniające poglądy polityczne
- dane ujawniające przekonania religijne lub światopoglądowe
- dane ujawniające przynależność do związków zawodowych
- dane genetyczne
- dane biometryczne (wykorzystywane w celu jednoznacznego zidentyfikowania osoby fizycznej)
- dane dotyczące zdrowia
- dane dotyczące seksualności lub orientacji seksualnej

Ludzie jednak często mówią w sieci o sobie zbyt dużo, bo liczą na to, że albo zobaczą pewne informacje wyłącznie znajomi, albo nikt się nie zorientuje, że to o nich właśnie chodzi. Zupełnie przy tym nie myślą, że nic tak naprawdę w sieci nie ginie, zawsze pozostaje jakiś ślad.

Nierozsądnym jest dzielenie się z ludźmi wiadomościami dotyczącymi naszych prywatnych spraw. Wyobrazić można sobie, co się stanie, gdy udostępnimy innym informacje na temat np. naszego stanu zdrowia, a konkretniej chorób, na które zapadamy. Otóż nie tylko zrezygnujemy z prywatności, ale też może okazać się, że firmy ubezpieczeniowe będą nam proponować wyższą kwotę ubezpieczenia na życie.

Jeżeli chcemy się zabezpieczyć przed wyciekiem danych, sami ich nie udostępniajmy. Im mniej informacji podajemy na swój temat w sieci, tym jesteśmy bardziej bezpieczni.

PAMIĘTAJ! Nie udostępniamy też innych informacji, np. numerów telefonów, PESEL, kont czy kart kredytowych, dowodów osobistych, czy adresów, a nawet w wielu sytuacjach adresów e-mail.

ZDJĘCIA

Aparaty fotograficzne wbudowane w telefony komórkowe pozwalają robić mnóstwo zdjęć, a aplikacje w tych samych telefonach umożliwiają natychmiastową ich publikację w sieci. Upublicznienie naszego życia staje się pokusą, szczególnie jeżeli dopadła nas już potrzeba bycia "lajkowanym" i "serduszkowanym". Można powiedzieć, że jest to swego rodzaju plaga internetu. Prawie w każdym drzemie potrzeba „pokazania się", zwrócenia na siebie uwagi. Na niej właśnie bazuje fenomen praktycznie wszystkich mediów społecznościowych. Jednak zaistnieć w cyfrowym świecie jest coraz trudniej. Zdjęć, które oglądamy każdego dnia tylko w mediach społecznościowych, są setki, a niekiedy nawet tysiące. Wrzucenie fotografii innej niż wszyscy staje się bardzo trudne. A tylko to, co nowe, świeże, kontrowersyjne lub nie do końca zgodne z prawem budzi zainteresowanie i podziw. Warto zatem zadać sobie pytanie, jak wiele jesteśmy w stanie zrobić dla kilku sekund popularności wśród znajomych… i jakie może mieć to dla nas konsekwencje w przyszłości. Kto, kiedy i w jakim celu wykorzysta zdjęcia wrzucone w chwili słabości, aby zaszkodzić naszej reputacji, karierze lub życiu osobistemu? Niestety chętni, aby to zrobić, na pewno się znajdą.

Podobnie jak nie udostępniamy danych wrażliwych czy poufnych, nie publikujemy zdjęć, które mogą zostać wykorzystane np. do ośmieszenia nas czy kradzieży.

Oto lista zdjęć, których raczej nie powinno się publikować w sieci:

- zdjęcia, na których jesteśmy niekompletnie ubrani,
- zdjęcia wnętrz mieszkań,

- zdjęcia drogich przedmiotów,
- zdjęcia z wakacji, gdy na nich właśnie przebywamy,
- zdjęcia z prywatnych spotkań.

CZYTAJ REGULAMINY!

Najważniejsze jest zazwyczaj to, co ukryte i trudne do wychwycenia „na pierwszy rzut oka". Nie wszystkie nasze dane trafiają tylko tam, gdzie mogłoby się nam wydawać. Dość często sami wyrażamy zgodę na to, aby nasze dane, które przesyłamy w jakieś miejsce w sieci lub udostępniamy określonej aplikacji lub serwisowi internetowemu, były udostępniane lub odsprzedawane innym osobom lub firmom. Informacje o tym znajdują się właśnie w regulaminach. Za każdym razem, gdy instalujemy nową aplikację na telefonie lub tablecie, rejestrujemy się do nowego serwisu czy usługi, należy uważnie przeczytać regulamin i zastanowić się, na co właściwie się zgadzamy. Niekiedy jest to trudne, gdyż regulaminy są zazwyczaj dość długie, a do tego napisane trudnym językiem. Zawiłość tych dokumentów jest oczywiście celowa. Nieświadomy swoich praw i zobowiązań użytkownik jest łatwiejszy do inwigilowania. A dane, które o nas zostaną zebrane, mają przecież swoją wymierną cenę, którą są gotowi zapłacić reklamodawcy, brokerzy informacji, a w niektórych państwach także i władze.

BEZPIECZNE HASŁA

Hasło to ciąg liter, liczb i znaków specjalnych, które służyć mają uwierzytelnieniu, czyli udowodnieniu, kim jesteśmy. Kiedy logujemy się do naszej poczty elektronicznej, bankowości online, dokonujemy zakupów albo uzyskujemy dostęp do rozmaitych urządzeń, korzystamy z haseł. W dzisiejszym świecie Internetu używamy ich w zasadzie bez przerwy. Hasło powinno być przez każdego właściciela chronione, czyli nie udostępniane osobom niepowołanym, ponieważ można narazić się na kradzież tożsamości lub pieniędzy albo utratę prywatnych danych.

Oprócz tego hasła można w zasadzie podzielić na dwa typy: słabe i silne. Słabe hasło to takie, które bardzo łatwo złamać, czyli cyberprzestępcy w prosty sposób będą mogli z Twoim loginem i hasłem skorzystać z Twojej bankowości online. Przykładam słabego hasła jest takie, które można łatwo odnaleźć w słowniku. Użytkownicy Internetu, aby łatwiej zapamiętać

hasła, używają na przykład imion swoich zwierząt i dodają do nich rok swoich urodzin. I tak popularnym hasłem jest np. "Burek 2005". Takie hasło można złamać w zasadzie w kilka sekund. Dlatego zaleca się tworzenie silnych haseł, czyli takich, których złamanie trwa znacznie dłużej, nawet kilka milionów lat. Oznacza to, że cyberprzestępca ma małe szanse na ich złamanie. Hasło silne nie jest słownikowym wyrazem, zawiera długi ciąg dużych i małych liter, cyfr i znaków specjalnych. Ponieważ normalnie trudno by było je zapamiętać, można pomóc sobie w taki sposób:

1. Przypominamy sobie wers jakiegoś ulubionego tekstu. My wybraliśmy *Pana Tadeusza* Adama Mickiewicza:
   Litwo! Ojczyzno moja! ty jesteś jak zdrowie
2. Pierwsze litery słów tworzą kombinację: **LOmtjjz**
3. Możemy zmienić wielkość liter, np: **lOMtjJz**
4. Do tego dodajemy znaki specjalne (mogą być takie jak w tekście literackim, ale sami coś również możemy dodać), np: **l!OM!tjJz** lub: **l!O$M!tjJz&**
5. Na końcu warto także dodać cyfry, np. **20l!O$M!tjJz&20**
6. Oto ostateczne hasło: **20l!O$M!tjJz&20**

Uwaga! Inwokacja i „Wlazł kotek na płotek…" to dwa najczęściej pojawiające się przykłady na różnych szkoleniach. Korzystając z tej metody, wybierzcie jakiś inny, mniej znany utwór.

Oczywiście można sprawdzić, czy nasze hasło jest silne. Wynik:

Źródło: howsecureismypassword.net

Jeżeli chcesz sprawdzić swoje hasło, skorzystaj z tej strony. Zielony kolor oznacza wysoki stopień bezpieczeństwa.

Ważne jest także, aby nie używać jednego hasła do wszystkich skrzynek czy urządzeń. Pamiętaj o tym, że cyberprzestępcy używają dziś programów komputerowych, które "wpuszczone" do naszych urządzeń złamią jedno hasło, a następnie sprawdzą, czy dostęp do innych stron nie jest zabezpieczony tym właśnie hasłem. Tak więc musisz mieć inne hasło do swojego banku, do portalu społecznościowego, do skrzynki mailowej itd. Hasło należy również zmieniać co jakiś czas, np. raz w miesiącu.

UWIERZYTELNIANIE DWUETAPOWE

Za każdym razem, gdy tylko pojawia się taka możliwość, warto skorzystać z uwierzytelnienia dwuetapowego podczas logowania lub potwierdzania różnych czynności wykonywanych w serwisach, gdzie bezpieczeństwo jest priorytetem (np. banki, poczta, serwisy społecznościowe). Uwierzytelnianie dwuetapowe polega na potwierdzeniu wykonywanego działania za pośrednictwem innego medium, np. operację przelewu bankowego robionego za pośrednictwem strony internetowej lub logowanie do poczty za pośrednictwem komputera należy potwierdzić dodatkowym kodem z SMS-s.

Najpopularniejsze formy dodatkowego uwierzytelnienia w świecie cyfrowym to potwierdzenie przy pomocy:

- kodu z uzyskanej wcześniej karty kodów jednorazowych (systemy bankowe coraz częściej odchodzą od tej formy, więc staje się ona archaiczna),
- kodu wysłanego SMS-em,
- potwierdzenia w aplikacji na smartfonie,
- potwierdzenie biometryczne (poprzez odcisk palca — linie papilarne lub poprzez Face ID — rozpoznanie twarzy).

NAWYKI I ZDROWY ROZSĄDEK

Istnieją trzy elementy, które zwiększają znacznie bezpieczeństwo w sieci. Są to:

- ochrona komputera, czyli zainstalowane oprogramowanie antywirusowe,
- wiedza człowieka, jak zachowywać się w sieci, co chronić, na jakie strony raczej nie wcho-

dzić, czego absolutnie nie otwierać i ściągać itd;

- nawyki, czyli zbiór prostych czynności, które powinny zostać wcielone w życie.

Najsłabszym z tych elementów są ludzkie nawyki, bo często komuś np. nie chce się wylogowywać z poczty czy nie myśli o tym, że publikacja zdjęcia może mu zaszkodzić.

Zawsze jednak warto kierować się zdrowym rozsądkiem. Jeżeli mamy wątpliwość, czy powinniśmy coś zrobić, poszukajmy najpierw wiedzy na ten temat, spytajmy osoby starsze, np. rodziców lub tego po prostu nie róbmy. I bądźmy czujni!

Ćwiczenie:

Połączcie się w pary i pracujcie metodą storytellingu. Wybierzcie jeden z poniższych scenariuszy i ułóżcie historię osoby, która:

a. Publikuje w sieci swoje zdjęcia, na których widać, jak chwali się bogactwem.

b. Publikuje w sieci zdjęcia swoich dzieci.

c. Publikuje w sieci swoje roznegliżowane zdjęcia.

Postarajcie się tak opowiedzieć historię, by pokazać konsekwencje takich działań.

Narzędzia niezbędne do wykonania ćwiczenia:
Komputer z programem do edycji treści lub kartka papieru A4 i coś do pisania: ołówek, długopis.

Ćwiczenie:

Z pomocą strony: **https://howsecureismypassword.net/** sprawdź, jak bezpieczne jest hasło do Twojej skrzynki pocztowej. Sprawdź również, jaka kombinacja cyfr, liter i znaków specjalnych jest potrzebna, by złamanie hasła do Waszego konta zajęło hakerom trylion lat.

Narzędzia niezbędne do wykonania ćwiczenia:
Komputer z dostępem do internetu, przeglądarka internetowa np. Mozilla Firefox, Chrome, Internet Explorer etc. W przeglądarce wpisz: **https://howsecureismypassword.net/**

Ćwiczenie:

Wyobraźcie sobie, że jesteście administratorami w grupie, do której należą wszystkie osoby z Waszej klasy. Ułóżcie w 10 punktach regulamin tej grupy. Zapiszcie w nim, co mogą robić uczestnicy forum, a czego im absolutnie zabraniacie. Wymyślcie sami nazwę grupy i cel jej

funkcjonowania w sieci.

Narzędzia niezbędne do wykonania ćwiczenia:

Kartki papieru A4, coś do pisania: ołówek, długopis etc.

Analiza narzędzi do komunikacji

Internet został wymyślony po to, by ludzie się porozumiewali szybciej, łatwiej, wygodniej i na duże odległości. Dlatego daje wiele okazji i narzędzi do komunikacji. Może to być komunikacja na linii człowiek-człowiek, człowiek-maszyna lub maszyna-człowiek. Są to zarówno skrzynki pocztowe, z których wysyłane są e-maile, jak i strony z chatami, programy do prowadzenia wideokonferencji, komunikatory służące do wysyłania krótkich informacji. Aby połączyć się z bliskimi z odległego krańca świata, zobaczyć ich na wielkim ekranie lub wspólnie uczestniczyć w oglądaniu filmu, wystarczy kilka kliknięć. Można też komunikować się ze stronami internetowymi w celu znalezienia jakichś informacji lub… inteligentnym odkurzaczem, aby posprzątał pod naszą nieobecność pokój lub kuchnię. Oprócz tego ludzie porozumiewają się w mediach społecznościowych, na blogach, portalach informacyjnych. Gdyby popatrzeć na Internet od strony filozoficznej, jest to przestrzeń do nieustannej wymiany myśli, zdań, poglądów i informacji. W tym miejscu interesować będzie nas jednak przede wszystkim komunikacja międzyludzka zapośredniczona przez maszyny podłączone do globalnej sieci.

W ostatnich latach najszybszą formą wymiany informacji są komunikatory. To programy komputerowe, które służą natychmiastowej wymianie informacji poprzez Internet. W komunikatorach ludzie wymieniają nie tylko informacje tekstowe, ale też zdjęcia, filmy, dokumenty, linki, emotikony, mogą prowadzić wideorozmowy. Znasz pewnie wiele komunikatorów. Do najpopularniejszych należą: Messenger, WhatsApp, Gadu-gadu, Signal. Są też rozbudowane systemy do komunikacji, prowadzenia konferencji, wspólnej pracy, wymiany plików. Z najpopularniejszych warto wymienić Teams wchodzący w skład pakietu biurowego Microsoft Office czy Hangouts Meet będący usługą Googla. W zależności od aktualnej mody jedne stają się bardziej popularne, inne zaś odchodzą w zapomnienie.

Tu interesować będzie nas przede wszystkim komunikacja międzyludzka. Jeżeli ma ona odbywać się w miarę bezpiecznie, należy pamiętać o kilku zasadach, które można podzielić

na dwie grupy:

1. Zasady zachowań ludzkich.
2. Zasady związane z technologią.

ZASADY KOMUNIKACYJNYCH ZACHOWAŃ LUDZKICH

Oto lista tych czynności, których na pewno nie powinno się robić:

- rozmowa z nieznajomymi, poza przypadkami uzasadnionymi (np. sprzedawcą w sklepie internetowym, profesorem z uczelni wyższej, od którego oczekujemy konsultacji, lekarzem itd). Wszystkie osoby, z którymi nawiązujemy kontakt nie powinny być anonimowe, tzn. znane z imienia i nazwiska. Podobnie i Wy, jeżeli nawiązujecie kontakt formalny, powinniście się przedstawić.
- wysyłanie nieznajomym plików, w tym zdjęć i filmów (w szczególności dotyczących naszej intymności, prywatności i rodziny),
- przesyłanie spamu, w tym tzw. łańcuszków szczęścia,
- otwieranie wiadomości z podejrzanymi linkami (mogą zawierać wirusy).

Ponieważ w tym typie komunikacji obowiązuje netykieta, pamiętać należy również o:

- niepisaniu całych zdań wielkimi literami, to oznacza, że krzyczymy, a nikt nie lubi, jak się na niego podnosi głos,
- używaniu emotikonek z rozsądkiem,
- nieprzeszkadzaniu osobie, która ma widoczny status: Zajęty,
- traktowaniu innych użytkowników sieci z należytym szacunkiem,
- komunikowaniu się w języku znanym rozmówcy, z uwzględnieniem wszystkich zasad poprawności językowej,
- duże załączniki przekazujemy za pośrednictwem chmury,
- szanuj prywatność innych
  (np. stosuj w komunikacji mailowej funkcję UDW — Ukryte Do Wiadomości),
- nie zmuszaj swego rozmówcy, aby musiał długo czekać na Twoją odpowiedź/reakcję,

- staraj się pisać konkretnie i zrozumiale, nie zawsze jest czas i miejsce na długie elaboraty.

Warto też pamiętać o tym, że to, jak się komunikujemy, świadczy o nas samych. Zanim napiszemy jakiekolwiek zdanie, zastanówmy się, jak może ono wpłynąć na nasz wizerunek w sieci i poza nią.

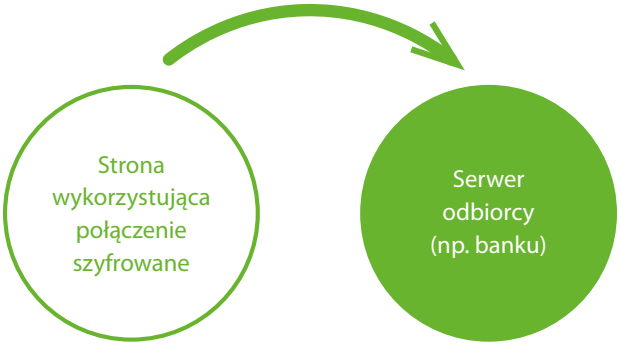
ZASADY ZWIĄZANE Z TECHNOLOGIĄ

Połączenia szyfrowane

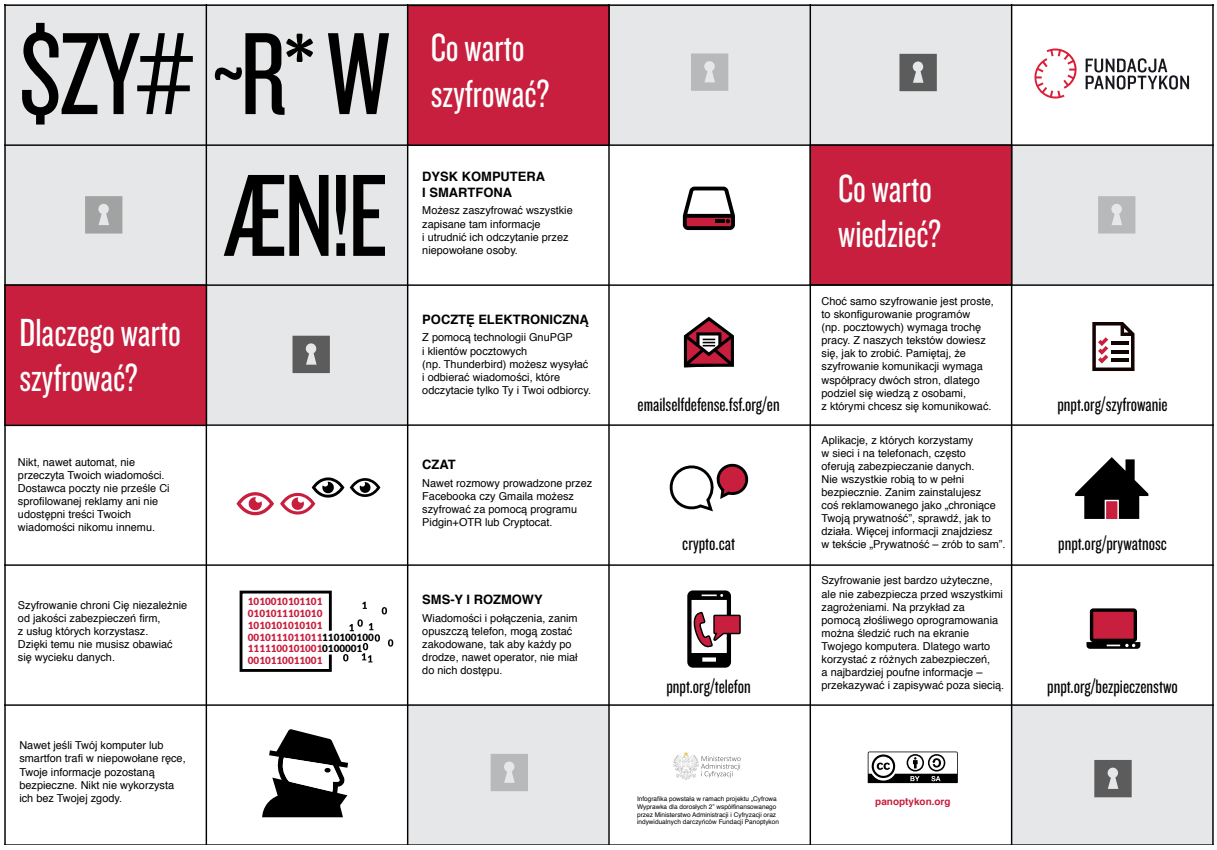
Po II wojnie światowej świat dowiedział się, że trzej Polacy: Marian Rejewski, Jerzy Różycki i Henryk Zygalski złamali kod Enigmy. Była to niemiecka maszyna szyfrująca, czyli urządzenie, które służyło do kodowania informacji przed jej wysłaniem. Zasady działania maszyn szyfrujących są dziś podobne — kodują one wiadomość, a właściwy odbiorca posiada klucz (lub maszynę odkodowującą), by móc odczytać informacje. Szyfrowanie jest czynnością, która służy zachowaniu poufności rozmowy. Zastanawialiście się kiedyś, dlaczego na kopertach jest klej? Odpowiedź jest banalna, aby móc zabezpieczyć list, który znajduje się w jej środku. Zaklejona koperta jest sygnałem, że nikt poza nami — adresatami listu nie czytał zawartej w niej wiadomości. Podobne funkcje pełniły w wiekach średnich (a także wcześniej) pieczęcie rodowe, które odciskało się w rozgrzanym wosku zabezpieczającym korespondencję. Gdy pieczęć była złamana, tajemnica korespondencji została naruszona, a posłaniec ukarany. Prawo do prywatności korespondencji jest niezbywalne i konstytucyjnie przysługuje każdemu obywatelowi. Do czasu, kiedy różnym instytucjom państwowym i komercyjnym nie wpadł do głowy pomysł, że to co ludzie piszą do siebie może być cennym źródłem informacji. W ślad za nimi poszli przestępcy internetowi, którzy z naszych rozmów mogą wyciągnąć wnioski, a ich celem jest zrobienie nam krzywdy.

UWAGA! Do szyfrowania przesyłanych wiadomości potrzebna jest chęć wszystkich stron uczestniczących w komunikacji.

JAK DZIAŁA POŁĄCZENIE SZYFROWANE?



Dlaczego i co warto szyfrować dowiecie się z poniższej infografiki.



Sprawdźcie, jak działają dwa najpopularniejsze i jedne z najbardziej bezpiecznych komunikatorów na rynku. Być może wybierzesz jeden z nich i zaczniesz w pełni korzystać z szyfrowanych, bezpiecznych połączeń.

whatsapp.com

signal.org

Kiedy korzystasz z poczty, banku lub sklepu internetowego oraz wszystkich stron, na których musisz podać swoje dane (login i hasło), sprawdzaj, czy połączenie jest szyfrowane.

Adres w pasku adresu powinien zawierać kłódkę i napis: **https** (“S” oznacza secure, czyli bezpieczny). Oczywiście jest to dziś konieczność jednak… Należy pamiętać, że ze względów bezpieczeństwa praktycznie wszystkie strony posiadają dziś to rozszerzenie, nawet te phisingowe. Inaczej nie mają one możliwości współpracy choćby z przeglądarką Googla (i innymi także).

Litera „s” w protokole oznacza jedynie rodzaj połączenia pomiędzy użytkownikiem a stroną. O samej stronie nic nam nie mówi.

PROGRAM ANTYWIRUSOWY

Coraz częściej z różnymi usługami online komunikujemy się za pośrednictwem zainstalowanych w smartfonach aplikacji. Oczywiście jeżeli są to aplikacje np. bankowe lub pocztowe posiadają one dość solidne zabezpieczenia także związane z szyfrowaniem danych. Jednak odrębnym problemem jest… przejęcie wpisywanych przez nas loginów i haseł przez szkodliwe oprogramowanie. Dlatego tak ważne jest, aby nie tylko komputery, ale i smartfony chronić odpowiednim oprogramowaniem, które ułatwia identyfikację zagrożenia wirusowego i pozwala te wirusy skutecznie zwalczać.

Ćwiczenie:

Stwórzcie kampanię promocyjną komunikatora opartego na połączeniach szyfrowanych.

Trzy grupy:

- G1 — tworzy 3 posty,
- G2 — projektuje plakat,
- G3 — projektuje billboard.

Narzędzia niezbędne do wykonania ćwiczenia:
Kartki papieru A4 (do napisania postów), coś do pisania: ołówek, długopis etc. Kartki A3 lub A2 (do plakatów i billboardów), coś do rysowania: kredki, mazaki, farby plakatowe.

Ćwiczenie:

Wersja nr 1: stwórzcie przewodnik po narzędziach do komunikacji dla sąsiada (w formie cyfrowej lub analogowej).

Wersja nr 2: stwórzcie przewodnik po narzędziach do komunikacji dla seniora (w formie

cyfrowej lub analogowej).

Narzędzia niezbędne do wykonania ćwiczenia:
Komputer z programem do edycji treści lub kartka papieru A4 i coś do pisania: ołówek, długopis.

Dobre praktyki zastosowań narzędzi do komunikacji

WIDEOKONFERENCJE

Wideokonferencja to rodzaj komunikacji multimedialnej, która odbywa się za pomocą komputerów, ale też smartfonów, czy tabletów. Polega na przesyłaniu z dużą szybkością obrazu i dźwięku w czasie rzeczywistym między nadawcą a odbiorcą (te role są zmienne) znajdującymi się w odległości od siebie. W takiej komunikacji wymieniane są między osobami dźwięk i obraz, ale nowoczesne programy pozwalają też na wymianę plików, prezentacji, filmów itd. Większość tego typu połączeń można nagrać, aby później móc do nich wrócić, np. żeby sobie przypomnieć poczynione w nich ustalenia lub aby udostępnić je osobom, które nie mogły w nich uczestniczyć. Tego typu rozwiązania znacznie usprawniają pracę zespołową. Sami przecież wiecie, że gdy macie do wykonania projekt zespołowy, trudno niekiedy ustalić termin spotkania, który wszystkim by odpowiadał. W wideokonferencji można zaś uczestniczyć praktycznie z każdego miejsca na Ziemi, podobnie zresztą jak ponownie odtworzyć jej zapis. Ponadto, jakby to powiedział Juliusz Słowacki, *chodzi o to, aby język giętki, powiedział wszystko, co pomyśli głowa*. Czasami trudno nasze myśli „ubrać" w słowa, łatwiej pokazać jest coś na przykładzie lub narysować. Narzędzia do wideokonferencji i taką możliwość dają swoim użytkownikom.

Przykładem takiego narzędzia jest np. Skype, Teams lub Google Hangouts. Pozwalają one na bezpłatne prowadzenie wideokonferencji przez Internet oraz płatne rozmowy z telefonami stacjonarnymi i komórkowymi. Poczytajcie więcej na ich temat, a jeżeli uznacie, że są one przydatne, wykorzystajcie je w codziennej pracy i nauce.

skype.com

products.office.com/pl-pl/microsoft-teams

hangouts.google.com

MESSENGER

To wciąż najpopularniejszy komunikator na cyfrowym rynku. Pozwala na wymianę wiadomości tekstowych oraz prowadzenie wideokonferencji. Oprócz tego osoby mogą wymieniać pliki, wysyłać emotikony, prowadzić rozmowy grupowe. Jego dostępność jest ogromna, a połączenie z Facebookiem (największym medium społecznościowym na świecie) ułatwia wyszukiwanie użytkowników i kontakt z nimi za pośrednictwem kilku kliknięć. I tak łatwo połączyć się z niewidzianym od lat znajomym lub znajomą, czy zaprosić do rozmowy koleżankę lub kolegę z równoległej klasy. Jednak jest jeden problem. Facebook, a właściwie jego właściciel Mark Zuckenberg, miał wiele wpadek na polu gospodarowania danymi użytkowników oraz współpracą z różnymi agendami rządowymi. Zakres zaufania dotyczący oferowanego produktu powinien być zatem ograniczony, tym bardziej, że oferowane w komunikatorze połączenia nie są szyfrowane.

E-MAIL

E-mail to inaczej list elektroniczny, czyli wiadomość tekstowa, do której mogą być dołączone pliki. Na skrzynce pocztowej możesz np. gromadzić wiadomości, tworzyć foldery, archiwizować wiadomości, tworzyć listę adresową. Skrzynkę e-mail zakłada się na największych portalach, takich jak: Onet, WP, Google itd. Ze względu na jego niekiedy formalny

charakter jest rodzajem dokumentu. Oczywiście nie dotyczy prywatnej korespondencji rozwijanej w formie listów pomiędzy prywatnymi użytkownikami Internetu. Choć jest to rodzaj komunikacji internetowej, rządzi się podobnymi prawami jak niegdyś tradycyjne listy. Zainteresowanych sztuką pisania listów odsyłamy do koncepcji Stefanii Skwarczyńskiej, tu wskażemy tylko kilka zasad, których należy się trzymać, aby nie popełnić rażącej gafy.

W komunikacji listownej obowiązują pewne zasady. Przede wszystkim:

- nie zaczynaj listu od słowa „Witam", jest to niegrzeczne, podobnie jak kończenie go zwrotem „Żegnam",
- używaj uniwersalnych formuł wstępu: „Dzień dobry" lub „Szanowna Pani/Szanowny Panie",
- używaj uniwersalnych formuł zakończenia: „Pozdrawiam" lub „Z wyrazami szacunku",
- pisz poprawnie, nie popełniaj błędów ortograficznych i interpunkcyjnych,
- nadawaj tytuły wiadomościom, to ułatwia ich porządkowanie,
- zwracaj się do odbiorcy z użyciem wielkiej litery: Ci, Tobie, Twoim,
- nie nadużywaj wielkich liter,
- nie nadużywaj formatowania (różne kolory, różne kroje i wielkości czcionek).

PRACA W ZESPOLE

Praca w zespole niekiedy niesie ze sobą wiele problemów. Jedna osoba poinformowała o jakichś działaniach drugą i poprosiła, aby przekazała informacje wszystkim członkom grupy. Ale ta druga zapomniała, a osoba trzecia i czwarta wykonały tę samą pracę co pierwsza, a pozostałe części zadania pozostały nietknięte. A zbliża się termin oddania pracy… Aby uniknąć takich nieporozumień w pracy zespołowej, warto skorzystać z rozwiązań, jakie dają tablice do efektywnego zarządzania zespołem. Pozwalają one na przejrzyste rozplanowanie pracy, przydzielanie zadań, ustalenie terminów i komunikację pomiędzy osobami należącymi do grupy. Tego typu produktów na rynku jest kilka, najpopularniejsze z nich to Trello, Asana i Slack. Doskonale nadaje się do tego także program Teams, o którym pisaliśmy przy okazji wideokonferencji. Które rozwiązanie będzie dla Was najlepsze, musicie sprawdzić sami.

trello.com

slack.com

asana.com

Jak trafiają do nas wirusy, czyli dobre praktyki w bezpiecznym korzystaniu z narzędzi online

MAILE I ZAŁĄCZNIKI

Aby zainfekować jak największą liczbę komputerów i telefonów, cyberprzestępcy często posługują się pocztą e-mail do dystrybucji złośliwego oprogramowania. Wirusy trafiają do nas, gdy otwieramy pocztę od nieznajomych. Najczęściej są to załączniki, które wcale mogą nie wyglądać groźnie. Schemat jest zazwyczaj podobny. Po zainfekowaniu jednego komputera wirus automatycznie rozsyła się do wszystkich adresatów, których mamy zapisanych w książkach adresowych. W ten sposób wprawiona zostaje w ruch samonakręcająca się machina. Otwarcie zawirusowanego maila przez jednego użytkownika powoduje rozesłanie go do wielu innych. Dzięki temu przestępcy mają szansę zainfekować w krótkim czasie olbrzymią liczbę komputerów w skali globalnej.

Dlatego tak ważne, choć dotyczy to przede wszystkim dorosłych, aby w sposób zgodny z przeznaczeniem korzystali z poczty służbowej i prywatnej. Atak na pocztę prywatną spowoduje, że zagrożeni zostaną wszyscy znajomi, których adresy przechowywane były

w książce adresowej oraz np. systemy obsługi sklepów internetowych, z którymi korespondowaliśmy, robiąc prywatne zakupy w Internecie. Jeżeli wirus zainfekuje konto jednej osoby, istnieje bardzo duże prawdopodobieństwo, że szybko rozprzestrzeni się po całej organizacji. Wiadomo przecież, że maile od współpracowników należy czytać, szczególnie jeżeli zostały one wysłane przez szefa lub szefową.

Zobaczcie w filmie *Anatomia ataku ransomware*, w jaki sposób często dochodzi do ataku hakerskiego rozpoczynającego się właśnie od przesłania zawirusowanego emaila: **youtube.com/watch?reload=9&v=HwqVv94ODgU**

Cyberprzestępcy często podszywają się także pod różne instytucje. Zazwyczaj są to maile od instytucji wysokiego zaufania społecznego np.: banku, ministerstwa, dystrybutora gazu lub prądu, szkoły, uczelni, instytucji charytatywnej, państwowej lub religijnej. Niekiedy są to wiadomości wyglądające, jakby nadane zostały przez firmy, z którymi wcześniej mieliśmy kontakt, np. sklepy internetowe, dostawców usług rozrywkowych. Właśnie to wspomniane zaufanie powoduje, że często bezrefleksyjnie otwieramy takie wiadomości, automatycznie przyczyniając się do ich dalszej dystrybucji bądź narażając się na utratę ważnych danych, dotyczących np. logowania do jakiejś usługi (bank, poczta). Zdarzają się też wiadomości od instytucji, które w rzeczywistości nie istnieją, a ich nazwy zostały wymyślone wyłącznie w celu popełnienia cyberprzestępstwa.

E-mail jest jedną z najczęściej wykorzystywanych przez przestępców dróg prowadzących do zawirusowania (w różnym celu) naszych komputerów i smartfonów.

Problem samoroznoszących się wirusów coraz częściej dotyczy nie tylko poczty internetowej, ale także różnego typu komunikatorów. Zawirusowane wiadomości przesyłane są do użytkowników komunikatorów połączonych często z mediami społecznościowymi. Po otwarciu przesłanej tą drogą zawirusowanej wiadomości automatycznie rozsyłana jest ona do wszystkich naszych znajomych z portalu społecznościowego. Skala szkód powodowanych rozprzestrzenianiem się wirusów poprzez korespondencję komunikatorową jest jeszcze większa niż w przypadku mailowej.

POBIERANIE PLIKÓW

Pobieranie plików z Chomikuj.pl lub innych seriwsów oferujących hosting plików, Torrenty i inne systemy wymiany plików pomiędzy użytkownikami to kolejne źródło, dzięki

któremu wirusy rozprzestrzeniają się w prosty i skutecznych sposób. Zazwyczaj od innych użytkowników (niezależnie od formy) pobieramy pliki z nielegalnie rozpowszechnionymi filmami, grami, programami, aplikacjami, książkami, a niekiedy także wciąż z muzyką. Jednak niestety nie zawsze dzieje się to bezinteresownie. Bo i kto bez wyraźnej korzyści narażałby się na nielegalną dystrybucję różnych tekstów kultury. Użytkownicy sieci, chcąc najczęściej zaoszczędzić i nie kupować oficjalnie wydanej płyty, płacić za obejrzenie filmu w serwisach VOD, kupować ebooka, gry czy programu, decydują się na ściągnięcie tzw. pirackiej wersji. Często są to pliki zawierające treści w tej samej jakości co oryginał. I równie często pobierając je z sieci na dysk komputera, infekujemy go wirusem dyskretnie dołączonym do pożądanego pliku.

Oprócz pliku zasadniczego (z filmem, piosenką itd.), które często spakowane są programem kompresującym, dołączony jest mały pod względem wielkości plik-wirus. Po rozpakowaniu paczki z tym, co rzeczywiście chcieliśmy pobrać, wirus aktywuje się na komputerze lub smartfonie.

Najprostszym rozwiązaniem jest oczywiście rezygnacja ze ściągania plików nieznanego pochodzenia. Jeżeli jednak już to robimy, przed rozpakowaniem nie zapomnijmy przeskanować ich programem antywirusowym.

INSTALOWANIE OPROGRAMOWANIA

Oprogramowanie, z którego korzystamy na naszych komputerach i smartfonach, a także innych urządzeniach podłączonych do sieci, powinno być zawsze aktualne. Przydaje się to choćby dlatego, że producenci oprogramowania w różnych aplikacjach „łatają" dziury, przez które przestępcy mogliby się dostać do naszych urządzeń. Dotyczy to przede wszystkim oprogramowania systemowego, ale także różnych programów i aplikacji użytkowych. Uaktualnienia powinny wejść nam w nawyk i, pod względem bezpieczeństwa, rozsądniej raczej zaufać producentowi oprogramowania. Choćby ze względu na prestiż swój i swego produktu będzie on starał się zabezpieczyć go w sposób najlepszy z możliwych.

Pamiętajmy jednak o jednym, aczkolwiek bardzo ważnym zastrzeżeniu! Jeżeli dokonujemy aktualizacji oprogramowania, o którą zostajemy poproszeni w pojawiającym się na ekranie komputera lub smartfona komunikacie, zawsze należy robić to, pobierając wspomnianą aktualizację z oficjalnej strony producenta bądź dystrybutora. Nigdy zaś nie należy klikać w link w wyskakującym okienku (pop-upie) z informacją, aby pilnie zainstalować,

zaktualizować bądź wykonać inną czynność ingerującą w działanie naszego sprzętu. Takie wyskakujące okienka często są pułapką. Linki, które są w nich zawarte, uaktywniają ściganie na nasz komputer pliku. Kiedy my jesteśmy przekonani, że jest to np. plik instalacyjny lub aktualizacyjny, tak naprawdę ściągamy do siebie złośliwe oprogramowanie.

Szczególną ostrożność w kwestii pobierania pliku instalacyjnego bądź aktualizacyjnego należy zachować w przypadku różnych programów antywirusowych.

Ćwiczenie:

Narysujcie w zespołach typowego hakera lub np. wyklejcie skojarzenia z nim związane w formie kolażu z gazet, wydrukowanych zdjęć i ikon tematycznych.

Narzędzia niezbędne do wykonania ćwiczenia:
Kartki A3, kolorowe czasopisma ze zdjęciami ludzi lub zdjęcia osób, nożyczki, klej.

Jak bezpiecznie przechowywać pliki i dane

Przechowywanie danych i plików to temat rzeka. Można go porównać do sensu posiadania domowego sejfu lub konta w banku szwajcarskim. Jeżeli kogoś na to stać (i ma co do tego sejfu włożyć), pewnie nie ma powodów, aby takowe zabezpieczenia posiadał. Z danymi i plikami jest nieco prościej, gdyż ich przechowywanie nie wymaga dużych nakładów finansowych, a czasami jest nawet bezkosztowe. Za to wartość plików i danych czasami bywa trudna do wycenienia. Nie można bowiem powiedzieć, ile wart jest projekt zapisany jedynie na dysku komputera, który zepsuł się na kilka godzin przed oddaniem go do oceny. Na pewno posiadanie kopii plików jest rozsądne. Nigdy nie wiemy, co może nam się przydarzyć i kiedy różne pliki będą nam w życiu potrzebne.

Jeżeli chodzi o przechowywanie danych zazwyczaj mówimy o dwóch możliwych rozwiązaniach. Idealnym miejscem na pliki jest bowiem:

- Nośnik zewnętrzny
- Chmura

Zastanówmy się teraz przez chwilę nad zaletami i wadami obu rozwiązań. Jednak zanim do tego przejdziemy, niech wybrzmi wskazówka zasadnicza: **Kopie plików, szczególnie**

tych cennych, najlepiej przechowywać na nośnikach zewnętrznych i w chmurze — jednocześnie.

NOŚNIKI ZEWNĘTRZNE

Nośniki zewnętrzne to dziś przede wszystkim pendrivy i przenośne dyski zewnętrzne. Jeszcze kilka lat temu najpopularniejszymi nośnikami były płyty CD i DVD. Jeszcze kilka lat wcześniej wszyscy korzystali z dyskietek. Jak widzicie, wraz z rozwojem technologii zmieniają się także sposoby archiwizowania naszych plików (czyli w pewnym sensie owoców naszej pracy). Jak pokazała historia, proces odświeżania archiwów plików powinien być systematyczny. Jeżeli bowiem dziś ktoś chciałby skorzystać z pliku, który dwadzieścia kilka lat temu zapisał na dyskietce… pewnie trudno byłoby mu znaleźć komputer z wejściem na dyskietkę (zakładając, że po latach wciąż byłaby ona sprawna). Podobnie za chwilę będzie z płytami CD i DVD, pomijając sposób ich przechowywania w określonej temperaturze, wilgotności i poszanowania (żeby się nie porysowały). Należy tu pamiętać, że każdy nośnik danych ma określoną żywotność (nowoczesne dyski SSD powinny pracować ok. 10 lat).

Oprócz tego, że wraz ze zmianami technologicznymi trzeba zmieniać swoje nawyki przechowywania danych, należy także zadbać o podstawowe zasady bezpieczeństwa. Rozważmy teraz, co może stać się z przykładowym pendrivem zawierającym jedyną kopię jakiś ważnych plików.

- Może zostać zgubiony, co jest o tyle prawdopodobne, że jest zazwyczaj dość małych rozmiarów (fizycznie).
- Może zostać skradziony, np. razem z kluczami lub portfelem, w którym go przechowujemy, aby zawsze mieć go ze sobą.
- Może zostać zawirusowany, np. gdy skorzystamy z publicznego komputera, damy innej osobie, aby coś z niego wzięła lub na nim zapisała (pani w punkcie drukarskim, kolega, współpracownik). W konsekwencji, gdy zawirusowany pendrive włożysz do swojego komputera, także i on zostanie zainfekowany.

Pamiętaj! Port USB, do którego podpinasz swój pendrive, to najprostsza droga do zawirusowania komputera. Zeskanuj pendrive przed podłączeniem do komputera programem antywirusowym.

W CHMURZE

Przechowywanie danych w chmurze zawsze budziło pewne wątpliwości. Dotyczyły one przede wszystkim bezpieczeństwa. Nie możemy mieć pewności, gdzie znajduje się serwer, na którym przechowywane są nasze dane. Nie wiemy, czy przestępcy nie postanowią go zniszczyć, uniemożliwić do niego dostęp lub wykraść z niego nasze pliki. Nie wiemy też, kto oprócz nas ma dostęp do przechowywanych tam danych. Każdy z operatorów chmury zapewnia o najlepszych z możliwych zabezpieczeniach. Jednak, jak pokazuje historia, nie ma zabezpieczeń, których w końcu nie udałoby się złamać. Co do dostępu do treści pewnie nikt nie może odpowiedzieć w pełni na pytanie, kto może je zobaczyć. Związane jest to choćby z bezpieczeństwem narodowym poszczególnych państw i współpracy operatorów z organizacjami rządowymi. Te zaś zazwyczaj są ściśle tajne. Nie rozwiejemy tu wszystkich wątpliwości i nie odpowiemy jednoznacznie, czy i z jakiej chmury korzystać. Decyzję każdy musi podjąć sam.

Google One one.google.com	W tej chmurze z usługą Googla połączonych jest wiele innych usług, a posiadanie przestrzeni dyskowej do przechowywania materiałów graficznych znacznie ułatwia np. wspólne projektowanie prezentacji.	
Dropbox dropbox.com	Oferuje 2GB bezpłatnej przestrzeni dyskowej. Dropbox był jedną z pierwszych takich usług na rynku i to właśnie jemu zawdzięczamy popularność przechowywania danych w chmurze.	
OneDrive onedrive.live.com	Oferowana jest użytkownikom pakietu Microsoft, czyli wszystkim użytkownikom Windowsa, przestrzeń na swoich serwerach. Usługa połączona jest z produktami pakietu Office.	

Zapamiętaj!

- **Niezależnie, gdzie przechowujesz swoje dane, pamiętaj, że są one bezpieczniejsze, gdy są zaszyfrowane.**
- **Im więcej kopii plików będziesz posiadał/a, tym większa szansa, że zawsze uda się je z któregoś źródła odtworzyć. Uwaga! Nie można popadać też w przesadę!**

Co zrobić, gdy zaatakuje nas wirus?

Wirus to powszechna nazwa szkodliwego, niechcianego oprogramowania, które ktoś siłą zainstalował na komputerze lub innych urządzeniach podpiętych do sieci. Zaczerpnięcie nazewnictwa ze środowiska medycznego, nawiązującego do rozpowszechniania się choroby wynika z pewnego podobieństwa działania. Wirusy często rozprzestrzeniają się samoistnie (automatycznie), atakują wybrane ofiary, ale i postronnych mieszkańców cyfrowego świata, a do ochrony przed nimi potrzebne są dwa aspekty: technologiczny i ludzki. Technologiczną „szczepionką" na wirusy są programy antywirusowe. Ludzka jest świadomość zagrożenia i schemat bezpiecznych, „higienicznych" zachowań, mogących uchronić przed zainfekowaniem.

Nie można wskazać jednoznacznych wytycznych do określonego typu szkodliwego oprogramowania. Z jednej strony nie można panikować, bo uniemożliwiłoby to normalne funkcjonowanie w cyfrowym świecie. Z drugiej strony, trzeba mieć przynajmniej świadomość zagrożenia, aby zorientować się, że dotknął nas atak cyberprzestępców. Biorąc pod uwagę liczbę próbek nowego złośliwego oprogramowania, które każdego dnia pojawia się na rynku, można niestety przypuszczać, że przynajmniej kilka razy każdy z użytkowników sieci poddany był próbie ataku. Na szczęście nie wszystkie próby są skuteczne.

Pamiętajcie, że szkodliwe oprogramowanie w jakiś sposób musi dostać się do Waszych komputerów i innych urządzeń. Nikt nie będzie pytał, czy je chcecie czy nie, bowiem odpowiedź byłaby oczywista. Jest ono instalowane w sposób przemocowy, wbrew woli użytkowników.

Jest bardzo wiele wirusów dostosowanych do różnych systemów operacyjnych komputerów, smartfonów i różnych inteligentnych urządzeń podłączonych do Internetu. Tak, tak! Wirusy mogą zaatakować nie tylko Twój komputer lub smartfon, ale także lodówkę, żarówkę, odkurzacz, samochód… a nawet inteligentną zabawkę dla dziecka.

Istnieje kilka sposobów ochrony przed wirusami, jednak nigdy nie możemy mieć stuprocentowej pewności, że uchronimy nasze urządzenia przed zainfekowaniem. Aby lepiej chronić nasz sprzęt, zapoznajmy się najpierw z najpopularniejszymi rodzajami wirusów, z jakimi obecnie mamy do czynienia.

RODZAJE WIRUSÓW

Cross-site scripting

Cross-site scripting (XSS) to luka w zabezpieczeniu strony umożliwiająca hakerom umieszczenie szkodliwego skryptu na zaufanej stronie lub w zaufanej aplikacji, która powoduje zainstalowanie złośliwego oprogramowania w przeglądarkach użytkowników. Za pomocą tej techniki hakerzy raczej nie atakują ani nie przekierowują użytkowników, lecz po prostu przesyłają swoje złośliwe oprogramowanie dużej grupie osób.

Źródło: avast.com/pl-pl/c-xss

Choć ta metoda rozprowadzania złośliwego oprogramowania wymaga sporych umiejętności informatycznych staje się coraz bardziej popularna.

Koń trojański

W epickim poemacie Wergiliusza pt. *Eneida* sprytny Odyseusz opracowuje plan, aby wprowadzić swoich żołnierzy do otoczonej murami obronnymi Troi. Zamiast burzyć mury lub wspinać się po nich, Odyseusz znalazł inną drogę: podstęp. Żołnierze trojańscy obserwowali, jak Grecy zdają się odpływać, zostawiając olbrzymiego drewnianego konia na znak kapitulacji. Świętujący zwycięstwo Trojanie przyciągnęli konia do miasta, a wraz z nim ukrytych w środku Odyseusza i jego żołnierzy.

Podobnie jak drewniany koń z poematu, konie trojańskie lub po prostu trojany to oszustwa i metody inżynierii społecznej, zachęcające niczego niepodejrzewających użytkowników do uruchamiania pozornie łagodnych programów komputerowych, które ukrywają jednak złośliwy kod.

Źródło: pl.malwarebytes.com/trojan, więcej na temat: avast.com/pl-pl/c-trojan

Robak

Robaki komputerowe to zagrożenia, które mogą same się powielać i spowalniać drastycznie Twój komputer.

Źródło: avast.com/pl-pl/c-computer-worm

Program szpiegujący

Spyware to rodzaj oprogramowania, które trudno wykryć. Gromadzi informacje na temat Twoich zwyczajów, surfowania w Internecie, historii przeglądania lub poufne dane (takie jak numery kart kredytowych), często korzysta z Internetu, aby przekazać te informacje osobom trzecim bez Twojej wiedzy.

Źródło: avast.com/pl-pl/c-spyware, więcej na temat: pl.malwarebytes.com/spyware

Malware

Malware (skrót od "malicious software") jest uważany za uciążliwy lub szkodliwy typ oprogramowania, który ma na celu potajemnie uzyskać dostęp do urządzenia bez wiedzy użytkownika. Rodzaje złośliwego oprogramowanie obejmują oprogramowanie szpiegujące (spyware), adware, phishing, wirusy, trojany, rootkity, zagrożenia typu ransomware oraz porywaczy przeglądarki.

Źródło: avast.com/pl-pl/c-malware

Adware

Adware to rodzaj wolnego oprogramowania wspieranego przez reklamy, które pojawiają się w wyskakujących oknach lub na pasku narzędzi na komputerze lub w przeglądarce. Większość adware jest denerwująca, ale nie jest niebezpieczna. Jednak niektóre z tego typu zagrożeń zbierają Twoje prywatne informacje, śledzą strony, które odwiedzasz, a nawet rejestrują sekwencje klawiszy.

Źródło: pl.malwarebytes.com/adware, więcej na temat: pl.malwarebytes.com/adware

Rootkit

Jakbyś się czuł, gdyby ktoś miał dostęp do Twojego komputera bez Twojej wiedzy? Niestety w przypadku rootkita to możliwe, może on zostać zainstalowany razem z różnymi rodzajami produktów i może zostać wykorzystany do zdalnej kontroli urządzenia.

Źródło: avast.com/pl-pl/c-rootkit

Keylogger

Keylogger jest to rodzaj oprogramowania szpiegującego, które potajemnie rejestruje naciśnięcia klawiszy, więc złodzieje mogą uzyskać informacje o Twoim koncie, kartach kredytowych, nazwy użytkowników, hasła i inne dane osobowe.

Źródło: avast.com/pl-pl/c-keylogger

Pamiętaj, że skoro każde wciśnięcie klawisza jest rejestrowane, przestępcy uzyskują dostęp do wszystkiego, co wpisujesz na swoim komputerze. Mogą także poznać np. prywatne plany związane z podróżą, o której rozmawiasz z bliskimi za pośrednictwem komunikatora.

Sniffer

Sniffery przybierają różną postać. Są między innymi sniffery pakietowe, Wi-Fi, sieciowe czy IP. Wszystkie jednak mają jedną wspólną cechę – są to programy, które przechwytują wszystkie dane przepływające pomiędzy komputerem a siecią, z którą jest on połączony.

Źródło: avast.com/pl-pl/c-sniffer

Ransomware

Oprogramowanie ransomware (znane również pod nazwą rogueware lub scareware) ogranicza dostęp do systemu komputerowego i wymaga zapłacenia okupu, aby blokada została usunięta. Najbardziej niebezpieczne ataki typu ransomware zostały spowodowane przez złośliwe oprogramowanie WannaCry, Petya, Cerber, Cryptolocker i Locky.

Źródła: avast.com/pl-pl/c-ransomware, pl.malwarebytes.com/ransomware

Pamiętajcie, aby nie ulegać szantażowi i nie płacić okupu. Czasami wystarczy po prostu reset komputera lub telefonu. Uleganie presji cyberprzestępcy może mieć kiepskie konsekwencje. Po wpłaceniu okupu komputer wcale może nie zostać odblokowany (blef), wysokość okupu może zostać podniesiona, możecie zostać uznani za osoby podatne na szantaż, które warto gnębić innymi atakami typu ransomware.

Robot internetowy

Bot lub komputer-zombie to urządzenie, które zostało zainfekowane szkodliwym oprogramowaniem, dzięki czemu cybeprzestępcy mogą mu wydawać różne polecenia. Najczęściej wykorzystują moc obliczeniową zainfekowanych komputerów do generowanie sztucznego ruchu w sieci. Komputery-zombie połączone w botnety mają np. za zadanie wchodzić na jakąś stronę internetową. Jeżeli tych wejść są miliony w tym samym czasie serwery, na których utrzymywane są atakowane strony, zostaną przeciążone i przestaną działać.

Więcej na ten temat przeczytacie tutaj: **plblog.kaspersky.com/botnet**

A co mogą robić boty o złym charakterze? Oto kilka przykładów:

- Boty mogą poszukiwać adresów e-mailowych, numerów telefonów, adresów

zamieszkania i innych danych osobistych opublikowanych na stronach internetowych.

- Zebrane informacje następnie mogą być sprzedane i użyte np. do spamowania.
- Można ich użyć również do kradzieży treści – po ściągnięciu treści oferowanych np. za opłatą bądź po obejrzeniu reklamy, udostępniane są one za darmo na pirackiej stronie.
- Boty są plagą wszelkich konkursów i stron, na których możemy się zarejestrować i otrzymać coś za darmo. Ktokolwiek próbował np. kupić bilety na popularny koncert lub wykorzystać opublikowany w sieci kod na darmową grę, wie, o czym mówimy.
- Boty – tym razem niezwiązane w WWW – są również wykorzystywane przez graczy w grach sieciowych.

Źródło: spidersweb.pl/2019/02/botnet-cybertarcza.html

Skoro już znamy możliwości różnych wirusów, zastanówmy się, jak możemy się przed nimi chronić i jak rozpoznać, że nasz sprzęt padł ofiarą cyberprzestępców. Skupmy się tu na dwóch urządzeniach, smartfonie i komputerze.

SMARTFON

Procesy bezpieczeństwa: objawy infekcji

Istnieje kilka objawów, po których można stwierdzić, że nasz telefon jest zainfekowany przez wirusa. Jeżeli zauważysz, że któryś z nich się nasila, postaraj się zeskanować swój smartfon programem antywirusowym. Jeżeli i to nie pomoże, konieczna będzie interwencja specjalisty-informatyka.

- Nieprzeciętnie wysokie rachunki za telefon,
- Nieprzeciętnie duże zużycie pakietu danych,
- Nieprawidłowe działanie aplikacji, częste zawieszanie się,
- Przegrzewanie się telefonu,
- Szybsze niż zwykle wyczerpywanie baterii,
- Często pojawiające się reklamy.

Zwróć uwagę, pisaliśmy o tym w rozdziale *Jak trafiają do nas wirusy*, jak ważny jest także czynnik ludzki, czyli rozważne i higieniczne korzystanie z cyfrowych dobrodziejstw za pośrednictwem smartfona.

Narzędzia

Istnieje wiele aplikacji, których celem jest ochrona antywirusowa smartfonów z różnymi systemami operacyjnymi. I tym razem nie wskażemy „najlepszego". Proponujemy kilka, z funkcjami których dobrze się zapoznać, aby wybrać dla siebie najlepszy produkt dostosowany do określonych potrzeb.

AVG Antywirus

Antywirus Mobilny Kaspersky

Avast Antywirus

ESET Mobile Security & Antivirus

Avira Antivirus

KOMPUTER

Wirusy komputerowe różnią się od siebie swoim działaniem. Także ich cele są różne i nie zawsze zrozumiałe dla przeciętnego użytkownika komputera. Nie ma jednej recepty, w której można rozpisać, jak zachować się, gdy zaatakuje nas wirus. To tak, jakby próbować leczyć się medykamentami, nie wiedząc, na co właściwie chorujemy. Można jednak spróbować ustalić wstępną ścieżkę postępowania, która może prowadzić nas do osiągnięcia celu. Pozbycia się złośliwego oprogramowania, ocalenia danych i ochrony prywatności. Przy czym zachowania prewencyjne są mimo wszystko bardziej istotne niż poszukiwanie rozwiązania, kiedy czasami jest już nieco zbyt późno.

Procesy bezpieczeństwa

- Nie wpadaj w panikę. Dopuszczenie skrajnych emocji do głosu uśpi zdrowy rozsądek. Nawet gdy obawiamy się, że wirus może poczynić nieodwracalne szkody, warto najpierw przeanalizować, co możemy zrobić, aby były one jak najmniejsze. Uleganie presji cyberprzestępców sprawi, że będą oni jeszcze bardziej zuchwali.
- Aby wirus nie rozprzestrzeniał się dalej, koniecznie odłącz komputer od Internetu. Uchronić to może także przed czynieniem przez wirusa różnych, czasami trudnych do odwrócenia, działań za pośrednictwem poczty, mediów społecznościowych, bankowości itp.
- Jeżeli Twój komputer podłączony jest do lokalnej sieci (domowej, szkolnej, firmowej), koniecznie odłącz go od niej, aby nie zainfekował innych sprzętów do tej sieci podłączonych.
- Jeżeli komputer przestał reagować na nasze polecenia lub nie chce się „normalnie" włączyć, spróbuj uruchomić go w trybie awaryjnym.
- Jeżeli komputer wciąż działa, spróbuj skopiować swoje dane. Być może szybka reakcja uchroni Cię przed ich utratą.
- Jeżeli dotychczas nie mieliście zainstalowanego programu antywirusowego, koniecznie spróbujcie zrobić to teraz. Najlepiej, jakby udało się to zrobić z zewnętrznego nośnika danych bez konieczności podłączania zawirusowanego komputera do sieci.
- Z poziomu innego, niezainfekowanego komputera zaktualizuj bazę wirusów we wspomnianym programie antywirusowym.

- Po wykonaniu powyższych czynności dokonaj pełnego skanowania komputera programem antywirusowym.
- Jeżeli wirus nie zostanie usunięty z komputera, nie bagatelizuj sytuacji i skontaktuj się z informatykiem, który pomoże w rozwiązaniu Twojego problemu.

Narzędzia

Istnieje bardzo wiele programów antywirusowych, które — przynajmniej deklaratywnie — są w stanie niemal całkowicie zabezpieczyć komputer. Jednak pamiętajmy o tym, że pomiędzy producentami tego oprogramowania trwa walka o klienta i niekończący się wyścig z przestępcami, którzy te programy chcą przechytrzyć. Zanim wybierzesz odpowiedni dla siebie produkt, dokładnie zapoznaj się z jego możliwościami, opłatami za jego użytkowanie i… opiniami innych użytkowników. Jeżeli nie możesz się zdecydować lub potrzebujesz profesjonalnej porady, skonsultuj swój wybór z informatykiem. Poniżej prezentujemy kilka wybranych, popularnych programów antywirusowych, z których ofertą warto się zapoznać. Pamiętajcie jednak, że poniższa lista nie wyczerpuje dostępnej i wciąż aktualizowanej oferty.

avast.com

kaspersky.pl

avg.com

bitdefender.pl

360totalsecurity.com

Pamiętaj! Niezależnie, czy ściągasz program antywirusowy na swój komputer czy na smartfon, zawsze korzystaj z oficjalnej strony producenta lub dystrybutora (sklep Google Play, App Store).

Ćwiczenie:

Przełóżcie wiedzę zdobytą na temat wirusów na baśń dla dzieci. Podpowiedzią będą dla Was linki:

https://plblog.kaspersky.com/fairy-tales-seven-young-goats/11293/

https://plblog.kaspersky.com/operation-puss-in-boots/11331/

https://plblog.kaspersky.com/fairy-tales-red-hood/11213/

Narzędzia niezbędne do wykonania ćwiczenia:
Komputer z dostępem do internetu, przeglądarka internetowa np. Mozilla Firefox, Chrome, Internet Explorer etc.

Kartki papieru A4, coś do pisania: ołówek, długopis etc.

Biblioteka pojęć:

TED

(Technology, Entertainment and Design – Technologia, Rozrywka i Design) – marka konferencji naukowych organizowanych corocznie przez amerykańską fundację non-profit Sapling Foundation. Celem konferencji jest popularyzacja – jak głosi motto – „idei wartych propagowania"

Konferencje TEDx są niezależne od TED, jednak stosują format analogiczny do tej konferencji. Mogą zostać zorganizowane przez kogokolwiek, kto otrzyma bezpłatną licencję od organizacji oraz będzie stosował się do ściśle określonych reguł. Konferencje nie mogą przynosić zysków, a koszty pokrywać mogą opłaty za wstęp lub sponsorzy. Prelegenci nie otrzymują wynagrodzenia i zgadzają się na publikację nagrania na koncie TEDx w portalu YouTube na licencji takiej samej, jak prelekcje TED oraz na ewentualny montaż nagrania i emisję na stronie TED.com.

Źródło: https://pl.wikipedia.org/wiki/TED_(konferencja)

Niebezpiecznik.pl

To jeden z najstarszych i najpopularniejszych rodzimych serwisów internetowych informujących o różnego typu zagrożeniach, które każdego dnia pojawiają się w cyfrowym świecie. Choć dziś zwraca uwagę komercyjny charakter firmy o tej samej nazwie co strona internetowa, to wciąż zdaje się być w czołówce portali promujących bezpieczeństwo w internecie.

Phishing

Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.

Źródło: https://pl.wikipedia.org/wiki/Phishing

Scam

Oszustwo polegające na wzbudzeniu u kogoś zaufania, a następnie wykorzystanie tego zaufania do wyłudzenia pieniędzy lub innych składników majątku. Osoba wzbudzająca fałszywe zaufanie zwykle działa na jedną z ludzkich cech charakteru, zarówno negatywnych, jak i pozytywnych, takich jak: pycha i chciwość, ale też empatia i altruizm.

Scam przybiera różne formy - począwszy od bezpośredniego wzbudzania zaufania poprzez kontakty osobiste, przez wysyłanie maili i tradycyjnych listów, po skomplikowane technicznie zabiegi z użyciem usług internetowych.

Źródło: https://pl.wikipedia.org/wiki/Scam

Nigeryjski szwindel

(Afrykański szwindel) – rodzaj spamu-oszustwa polegający na wciągnięciu ofiary w fikcyjny transfer wielkiej kwoty pieniędzy (rzędu kilku milionów USD) najczęściej z któregoś z krajów afrykańskich (początkowo głównie do Nigerii).

Źródło: https://pl.wikipedia.org/wiki/Nigeryjski_szwindel

Clone phishing

Typ phishingu, w którym prawdziwy e-mail posiadający załącznik lub link zostaje użyty przez przestępcę jako wzór przy tworzeniu wiadomości na potrzeby oszustwa. Załączniki lub linki zostają zastąpione złośliwymi wersjami, a następnie wysłane z adresu email sfałszowanego tak, aby wyglądał jak ten należący do oryginalnego nadawcy. Ta technika może zostać użyta pośrednio, przy pomocy wcześniej zainfekowanej maszyny do stworzenia następnej wykorzystując zaufanie społeczne do wnioskowanego adresu email, ponieważ obie strony otrzymują oryginalny email

Źródło: https://pl.wikipedia.org/wiki/Phishing

Whaling

Część ataków phishingowych została skierowana w szczególności do kierownictwa wyższego szczebla i innych ważnych celów z branży biznesowej. Z tego powodu ataki te nazwano whaling (z języka angielskiego „wielorybnictwo"). W przypadku ataków tego typu, sfałszowana witryna lub wiadomość jest tworzona z uwzględnieniem np. stanowiska ofiary w firmie. Treść e-maili często przypomina pisma pochodzące z kancelarii prawnych lub urzędów państwowych. Taka wiadomość może zawierać załącznik w postaci złośliwego oprogramowania i nakłaniać ofiarę do jego instalacji np. w celu uzyskania dostępu do ważnego dokumentu.

Źródło: https://pl.wikipedia.org/wiki/Phishing

Fałszywa pomoc techniczna

Metoda oszustwa internetowego, w której przestępca próbuje zastraszyć ofiarę i skłonić ją do zapłacenia za zbędną pomoc techniczną. Metoda ta wykorzystuje brak wiedzy informatycznej ofiary.

Oszuści prowadzący fałszywą pomoc techniczną mogą zadzwonić do ofiary, podając się za przedstawicieli producenta oprogramowania (np. Microsoftu). W innym wariancie ataku połączenie nawiązuje ofiara, nakłoniona przez komunikat zamieszczony na stronie

internetowej (czasami blokujący przeglądarkę i trudny do zamknięcia). Przestępcy proszą o zainstalowanie aplikacji dającej zdalny dostęp do urządzenia. Następnie mogą informować ofiarę o rzekomych problemach na komputerze, np. poprzez wskazywanie niegroźnych ostrzeżeń i błędów z systemowego podglądu zdarzeń lub „skanowanie" komputera komendą *tree* w wierszu poleceń. Ostatecznie oszust proponuje zakup pomocy technicznej, która ma wyeliminować rzekome usterki.

Źródło: https://pl.wikipedia.org/wiki/Fałszywa_pomoc_techniczna

Pharming

Bardziej niebezpieczna dla użytkownika oraz trudniejsza do wykrycia forma phishingu. Charakterystyczne dla pharmingu jest to, że nawet po wpisaniu prawidłowego adresu strony www, ofiara zostanie przekierowana na fałszywą (choć mogącą wyglądać tak samo) stronę WWW. Ma to na celu przejęcie wpisywanych przez użytkownika do zaufanych witryn haseł, numerów kart kredytowych i innych poufnych danych.

Źródło: https://pl.wikipedia.org/wiki/Pharming

SMS phishing

Atak socjotechniczny podobny do phishingu polegający na rozsyłaniu SMS-ów, które mają skłonić ofiarę do podjęcia określonego działania.

Źródło: https://pl.wikipedia.org/wiki/SMS_phishing

„Cookie"

(Ciasteczka) - wszystkie technologie, które przechowują i wykorzystują informacje na urządzeniu, na którym korzystasz z naszych Usług, np. na komputerze, tablecie lub telefonie komórkowym. Używamy na przykład plików cookie typu HTTP, które są niewielkimi plikami danych (zazwyczaj składającymi się z cyfr i liter), które pobierasz, kiedy zaczynasz korzystać z naszych Usług, i które pozwalają nam rozpoznać Twoje urządzenie. Używamy także technologii takich jak znaczniki pikselowe i pakiety oprogramowania osadzone w naszych aplikacjach.

Istnieją różne typu plików cookie, na przykład:

- Pliki cookie obsługiwane bezpośrednio przez Cisco („pliki cookie administratora") i pliki cookie obsługiwane w naszym imieniu, np. przez agencje reklamowe lub firmy analizujące dane („pliki cookie osób trzecich").
- Pliki cookie, które funkcjonują przez określony czas, w tym te, które funkcjonują jedynie

do czasu zamknięcia przeglądarki (tzw. „sesyjne pliki cookie"). Są one automatycznie kasowane po zamknięciu przeglądarki. Inne pliki tego typu to „trwałe pliki cookie", które nie są kasowane po zamknięciu przeglądarki. Służą one np. do rozpoznania Twojego urządzenia, gdy znów włączysz przeglądarkę internetową.

Źródło: https://www.cisco.com/c/pl_pl/about/legal/adct.html

Uwierzytelnianie wielopoziomowe

Sposób zabezpieczenia oraz autoryzacji podczas logowania przed skorzystaniem z konta użytkownika przez niepowołane osoby poprzez zdobycie przez nią identyfikatora użytkownika i hasła uwierzytelniającego. Oprócz podania tych danych logowania, użytkownik musi (w kolejnych etapach) podać uzyskany kod lub frazę np. ze swojego przenośnego urządzenia internetowego (np. smartfon, tablet), poprzez przepisanie go z e-maila wysłanego przez serwis, na którym użytkownik próbuje się zalogować, czy też za pomocą specjalnej karty, linii papilarnych palca itp

Źródło: https://pl.wikipedia.org/wiki/Uwierzytelnianie_wielopoziomowe

Hasła

Są jednym z podstawowych sposobów, w jaki możemy udowodnić, kim jesteśmy. Używając ich logujemy się do poczty elektronicznej, bankowości on-line, dokonujemy zakupów w sieci i uzyskujemy dostęp do urządzeń, takich jak laptop lub smartfon. Można powiedzieć, że w wielu przypadkach hasła są niczym klucze do naszego królestwa. W związku z tym, jeśli ktoś byłby w posiadaniu Twojego hasła, mógłby dokonać kradzieży Twojej tożsamości, transferu Twoich pieniędzy lub uzyskać dostęp do wszystkich Twoich prywatnych danych. Używanie silnych haseł jest niezbędne, aby chronić swoją tożsamość i swoje informacje. Dowiedzmy się, co sprawia, że hasło jest silne i jak bezpiecznie je stosować.

Silne hasła - Cyberprzestępcy opracowali wyspecjalizowane programy, które coraz lepiej potrafią odgadnąć, a mówiąc inaczej "złamać", hasła. To oznacza, że mogą oni wykraść Twoje hasła, jeśli są one słabe albo łatwe do odgadnięcia. Nigdy nie należy używać łatwo dostępnych informacji tworząc hasła. Do takich informacji należą na przykład data urodzenia, imię zwierzątka lub cokolwiek, co można łatwo znaleźć na portalach społecznościowych lub wyszukać w Google. Zamiast tego, najlepszym sposobem na stworzenie silnego hasła jest użycie długiego hasła, które im więcej znaków zawiera, tym lepiej. Najlepiej zamiast używać jednego słowa, używać wielu słów, a nawet pełnych zdań.

Źródło: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201305_po.pdf

Hakowanie

Proces łamania zabezpieczeń komputera w celu uzyskania do niego dostępu – zarówno w dobrych, jak i złych intencjach – natomiast crackowanie dotyczy przypadków o charakterze przestępczym. W ogólnym rozumieniu hakerzy budują, a crackerzy łamią, angażują się w taką działalność, jak wykradanie numerów kart kredytowych, instalacja wirusów, niszczenie plików lub gromadzenie danych osobowych w celu ich sprzedaży.

Źródło: https://www.avast.com/pl-pl/c-cracking

Zapora sieciowa

Jeden ze sposobów zabezpieczania sieci i systemów przed intruzami. Termin ten może odnosić się zarówno do sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do komputera, na którego straży stoi. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz, tzn. sieci publicznych, Internetu, chroni też przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz. Często jest to komputer wyposażony w system operacyjny (np. Linux, BSD) z odpowiednim oprogramowaniem. Do jego podstawowych zadań należy filtrowanie połączeń wchodzących i wychodzących oraz tym samym odmawianie żądań dostępu uznanych za niebezpieczne.

Najczęściej używanymi technikami obrony są:

- filtrowanie pakietów, czyli sprawdzanie pochodzenia pakietów i akceptowanie pożądanych,
- stosowanie algorytmów identyfikacji użytkownika (hasła, cyfrowe certyfikaty),
- zabezpieczanie programów obsługujących niektóre protokoły.

Bardzo ważną funkcją zapory sieciowej jest monitorowanie ruchu sieciowego i zapisywanie najważniejszych zdarzeń do dziennika (logu). Umożliwia to administratorowi wczesne dokonywanie zmian konfiguracji. Poprawnie skonfigurowana zapora powinna odeprzeć wszelkie znane typy ataków. Na zaporze można zdefiniować strefę ograniczonego zaufania – podsieć, która izoluje od wewnętrznej sieci lokalne serwery udostępniające usługi na zewnątrz.

Źródło: https://pl.wikipedia.org/wiki/Zapora_sieciowa

Chmura

Chmurę definiować można na dwa sposoby. Pierwszym z nich jest chmura obliczeniowa, z angielskiego cloud computing, drugim zaś chmura publiczna, tudzież dyski w chmurze,

oferowane przez największych potentatów świata IT, przez niezależne firmy czy organizacje oraz przez producentów sprzętu, komputerów, smartfonów, tabletów, a nawet przez firmy telekomunikacyjne.

Źródło: https://www.komputerswiat.pl/poradniki/internet/czym-jest-popularna-chmura/5nhxw4c

Wirus komputerowy

Program lub fragmentem kodu, przedostaje się do komputera bez Twojej wiedzy lub pozwolenia. Niektóre wirusy są tylko irytujące, ale większość wirusów jest destrukcyjna i przeznaczona do infekowania i przejęcia kontroli nad podatnymi systemami. Wirus może przenosić się między komputerami i sieciami poprzez kopiowanie się, podobnie jak wirus biologiczny przechodzi z osoby na osobę.

Wirusy są zwykle ukryte w powszechnie używanych programach, takich jak gry lub przeglądarki plików PDF, możesz też otrzymać zainfekowany plik w załączniku do wiadomości e-mail lub wraz z innym plikiem pobranym z Internetu. Jak tylko wejdziesz w interakcje z plikiem (uruchomisz program, klikniesz na załącznik lub otworzysz plik), wirus automatycznie się uruchomi. Kod może wtedy skopiować się do innych plików i dokonać zmian w Twoim komputerze.

Źródło: https://www.avast.com/pl-pl/c-computer-virus

Cross-site scripting (XSS)

Luka w zabezpieczeniu strony umożliwiająca hakerom umieszczenie szkodliwego skryptu na zaufanej stronie lub w zaufanej aplikacji, który powoduje zainstalowanie złośliwego oprogramowania w przeglądarkach użytkowników. Za pomocą tej techniki hakerzy raczej nie atakują ani nie przekierowują użytkowników, lecz po prostu przesyłają swoje złośliwe oprogramowanie dużej grupie osób.

Źródło: https://www.avast.com/pl-pl/c-xss

Koń trojański

Typ wirusa, który udaje, że jest użyteczny lub pomocny, podczas gdy w rzeczywistości uszkadza Twój komputer i kradnie dane.

Źródło: https://www.avast.com/pl-pl/c-trojan

Robaki

Programy, które same się powielają i rozprzestrzeniają się za pośrednictwem sieci komputerowej.

Źródło: https://www.avast.com/pl-pl/c-computer-worm

Malware

Różnego rodzaju szkodliwe programy, które usiłują zainfekować komputer lub urządzenie mobilne. Hakerzy wykorzystują malware do różnych celów — wykradania danych osobowych, haseł i pieniędzy oraz blokowania dostępu do urządzeń. Przed zagrożeniem typu malware można się uchronić, stosując odpowiednie zabezpieczenia.

Źródło: https://www.avast.com/pl-pl/c-malware

Spyware

Rodzaj złośliwego oprogramowania, które jest wykorzystywane przez hakerów do szpiegowania, aby zyskać dostęp do Twoich poufnych informacji, danych bankowych lub aktywności online. Pokażemy Ci, w jaki sposób możesz zabezpieczyć się przed szpiegowaniem.

Źródło: https://www.avast.com/pl-pl/c-spyware

Adware

Typ złośliwego oprogramowania bombardującego Cię niekończącymi się wyskakującymi oknami, które potencjalnie mogą być niebezpieczne dla Twojego urządzenia.

Źródło: https://www.avast.com/pl-pl/c-adware

Keylogger

Rodzaj oprogramowania szpiegującego, które potajemnie rejestruje naciśnięcia klawiszy, więc złodzieje mogą uzyskać informacje o Twoim koncie, kartach kredytowych, nazwy użytkowników, hasła i inne dane osobowe.

Źródło: https://www.avast.com/pl-pl/c-keylogger

Sniffer

Sniffery - przybierają różną postać. Są między innymi sniffery pakietowe, Wi-Fi, sieciowe czy IP. Wszystkie jednak mają jedną wspólną cechę – są to programy, które przechwytują wszystkie dane przepływające pomiędzy komputerem a siecią, z którą jest on połączony.

Źródło: https://www.avast.com/pl-pl/c-sniffer

Oprogramowanie ransomware

(Znane również pod nazwą rogueware lub scareware) - ogranicza dostęp do systemu

komputerowego i wymaga zapłacenia okupu, aby blokada została usunięta. Najbardziej niebezpieczne ataki typu ransomware zostały spowodowane przez złośliwe oprogramowanie WannaCry, Petya, Cerber, Cryptolocker i Locky.

Źródło: https://www.avast.com/pl-pl/c-ransomware

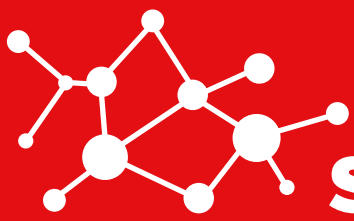
Botnet

Aplikacja, która wykonywała powtarzalne czynności w sieci – często tzw. web spidering czyli przeczesywanie sieci w celu jej archiwizacji bądź indeksowania. Większość takich robotów, a niektórzy szacują, że nawet połowa ruchu sieciowego jest ich dziełem, jest grzeczna i nie narusza zasad.

A co mogą robić boty o złym charakterze? Oto kilka przykładów:

- Boty mogą poszukiwać adresów e-mailowych, numerów telefonów, adresów zamieszkania i innych danych osobistych opublikowanych na stronach internetowych. Zebrane informacje następnie mogą być sprzedane i użyte np. do spamowania.
- Boty mogą być również użyte do sztucznego obciążania stron internetowych, np. w celu wyeliminowania konkurencji bądź usunięcia niewygodnej politycznie strony.
- Można ich użyć również do kradzieży treści – po ściągnięciu treści oferowanych np. za opłatą bądź po obejrzeniu reklamy, udostępniane są one za darmo na pirackiej stronie.
- Boty są plagą wszelkich konkursów i stron, na których możemy się zarejestrować i otrzymać coś za darmo. Ktokolwiek próbował np. kupić bilety na popularny koncert lub wykorzystać opublikowany w sieci kod na darmową grę, wie o czym mówię.
- Boty – tym razem niezwiązane w WWW – są również wykorzystywane przez graczy w grach sieciowych. Potrafią one albo reagować szybciej niż człowiek, dając nieuczciwemu graczowi pewną przewagę bądź są w stanie farmić te same treści przez całe godziny, bez znudzenia, zarabiając w ten sposób wirtualne złoto bądź przedmioty

Źródło: https://www.spidersweb.pl/2019/02/botnet-cybertarcza.html



sieć na kulturę

www.siecnakulture.pl

FUNDACJA **WSPIERANIA**
ZRÓWNOWAŻONEGO ROZWOJU