W drugim Cyber Poradniku radzimy Wam na jakie szczegóły zwracać uwagę oraz co zrobić, gdy padniemy ofiarą cyberprzestępstwa.

Żyjemy w czasach, w których na co dzień korzystamy z Internetu oraz nowoczesnych technologii. Te zdobycze współczesnego świata niosą za sobą jednak nowy rodzaj zagrożeń dla społeczeństwa, a mianowicie cyberprzestępstwa. Zgodnie z jednym z artykułów autorstwa dziennikarzy The Economist obecnie o wiele bardziej opłacalnym biznesem od przemysłu naftowego jest handel danymi natomiast nasze dane są cenniejsze od ropy. I to właśnie o takie informacje codziennie toczą się rozgrywki pomiędzy użytkownikami a cyberprzestępcami, niezależnie czy chodzi o dane osobowe czy dostępowe – każde z nich są dla cyberprzestępców cennym łupem. Dlatego właśnie tworzymy dla Was Cyber Poradnik i chcemy Was uświadamiać jak poprawnie się dbać o swoje dane w Internecie i chronić swoją prywatność. Niestety, nawet najlepsze zabezpieczenia nie są nam w stanie zagwarantować bezpieczeństwa w 100%. Zawsze istnieje ryzyko, że pewnego dnia staniemy się ofiarą przestępstwa internetowego.

Właśnie dlatego powstał dzisiejszy materiał – chcemy pokazać Ci jak zdiagnozować czy padłeś ofiarą cyberprzestępstwa, zaprezentować najczęściej występujące przesłanki co do tego czy Twoje dane zostały skompromitowane oraz jak zareagować w takiej sytuacji. W tym celu zebraliśmy garść przydanych porad, które przygotowali specjalnie dla Was nasi specjaliści. Mamy nadzieję, że pomogą Wam one zachować bezpieczeństwo oraz uświadomią jak postępować w przypadku wystąpienia incydentu bezpieczeństwa. Dzisiejszy materiał został podzielony na cztery bloki tematyczne dotyczące różnych prawdopodobnych wektorów przestępstwa. W każdym z nich pokazujemy, przesłanki co do tego czy mogłeś paść ofiarą ataku oraz proponujemy kilka zapobiegawczych środków jak zapobiec dalszej eskalacji problemu.

Na wstępie jednak chcemy Ci przypomnieć, że nawet jeśli stałeś ofiarą ataku to nie musisz się wstydzić tego faktu. Pamiętaj również, aby w takiej sytuacji zachować spokój i nie postępować pochopnie (tak wiemy to trudne). Jeśli uważasz natomiast, że nie jesteś w stanie samodzielnie poradzić sobie z problemem nie bój się prosić o pomoc i zasięgnąć jej u specjalistów z tej dziedziny. Na koniec artykułu po krótce prezentujemy Ci jak S.M.S. może pomóc w takiej sytuacji. Jednocześnie staraj się pamiętać, że mimo, że przestępstwa tego typu dzieją się w cyberprzestrzeni to mają one swoje konsekwencje w normalnym życiu i grozi za nie odpowiedzialność karna. Zawsze dochodź swoich praw w takich sytuacjach.

Co zrobić jeśli zostałeś naciągnięty przez nieuczciwego lub fałszywego sprzedawcę?

Jeśli przeczytałeś nasz poprzedni wpis to mamy już pewność, że wiesz jak rozpoznać fałszywy sklep i bezpiecznie robić zakupy przez Internet (jeśli jednak ominął Cię pierwszy numer Cyber Poradnika, koniecznie nadrób te braki). Niemniej może się zdarzyć, że przeoczymy niektóre przesłanki lub zostaniemy naciągnięci na niezwykle wiarygodnie wyglądający sklep internetowy i padniemy ofiarą oszustwa. Co w takim wypadku należy zrobić? Jak tylko zorientujesz się, że dokonałeś zakupów w fałszywym sklepie koniecznie poinformuj o tym fakcie swojego dostawcę płatności, czyli bank. Być może uda się jeszcze zatrzymać wykonaną transakcję. Następnie sklep możesz również zgłosić do odpowiedniej jednostki zajmującej się obsługą incydentów jak np. Policja. Dzięki temu możesz mieć pewność, że zostaną podjęte konkretne działania celem złapania sprawcy. Zostaw również swój komentarz na jednym z portali zbierających opinie o sklepach, aby ostrzec innych użytkowników sieci o istnieniu fałszywego sklepu lub sprzedawcy.

Jak zachować się w obliczu przejęcia Twojego konta?

Zakładamy, że posiadasz przynajmniej jedno konto na jakimś portalu w Internecie, dzięki któremu masz dostęp do różnorodnych usług – począwszy od bankowości elektronicznej, poprzez media społecznościowe, a skończywszy na platformach zakupowych. Ze względu na szeroki wachlarz funkcjonalności oraz informacji, które zawierają na nasz temat stają się „towarem" pożądanym przez cyberprzestępców. Jak rozpoznać, że ktoś mógł uzyskać dostęp do Twojego konta?

- **Logowanie.** Jeśli podczas standardowego logowania nie możesz uzyskać dostępu do konta (pomimo pewności, że wprowadzasz poprawne hasło) powinno zwrócić to Twoją uwagę. W tym miejscu zalecamy również wprowadzenie do logowania kolejnej metody uwierzytelniania podczas uzyskiwania dostępu do konta czyli tzw. **uwierzytelniania dwuskładnikowego**. Wtedy sama znajomość hasła dla atakującego nie będzie wystarczającą wartością do uzyskania dostępu do konta.
- **Wiadomości.** Twoi znajomości dostają od Ciebie wiadomości (np. na Facebooku czy Twitterze) lub e-maile, których nie jesteś autorem? To kolejny symptom tego, że Twoje konto mogło zostać skompromitowane.
- **Wyciągi.** W poprzednim wydaniu Cyber Poradnika pisaliśmy już na temat sprawdzania danych z wyciągów bankowych. To dobra metoda, aby mieć kontrolę nad swoimi wydatkami. Problem pojawia się natomiast wtedy, kiedy widzisz na nich transakcje,

o których nie masz najmniejszego pojęcia.
- **Ustawienia.** Jeśli na swoim koncie zauważysz zmiany w ustawieniach czy swoich danych, a nie ty ich dokonałeś może to się okazać działalnością ze strony osób trzecich.
- **Oświadczenia firm.** Zdarzają się masowe kompromitacje danych użytkowników różnych portali, które umożliwiają im założenie na nich konta. Jeśli strona, na której masz konto wydała oświadczenie o tym, że nastąpił wyciek danych jej użytkowników/klientów, załóż że również twoje informacje mogły dostać się w ręce cyberprzestępców.

Znasz przesłanki tego, czy mogło dojść do przejęcia Twojego konta. W takim razie teraz czas przedstawić co możesz zrobić, aby zapobiec eskalacji tego incydentu.

- **Sprawdź swoje konto.** Za pośrednictwem takich stron jak np. https://haveibeenpwned.com/ możesz sprawdzić, czy twój adres e-mail (za pomocą, którego zwykle zakładane są różne konta użytkownika) został udostępniony podczas jakiegokolwiek zarejestrowanego wycieku danych użytkowników.
- **Hasło.** Pamiętaj, żeby stosować różne hasła do każdego z kont użytkownika, które posiadasz. Zmniejszy to prawdopodobieństwo, że cyberprzestępca zdobędzie dzięki temu dostęp do wszystkich twoich kont (bo ma dostęp do Twojego e-maila oraz sprawdzi, czy zastosowałeś to samo hasło również na innych portalach). Jeśli stosujesz takie samo hasło w innych kontach, co w skompromitowanym serwisie natychmiast je zmień.
- **Logowanie.** Jeśli masz dostęp do konta, a obawiasz się, że mogło zostać skompromitowane natychmiast zmień hasło. Natomiast jeśli nie masz możliwości zalogowania się skontaktuj się z odpowiednią komórką danego portalu, odpowiedzialną za administrację danymi uwierzytelniającymi. Na każdej stronie powinien znaleźć się odnośnik/kontakt do takich zespołów. W razie problemów możesz wykorzystać również formularz kontaktowy, który może być udostępniony właśnie do zgłaszania takich spraw.
- **Ponowny dostęp.** W momencie, kiedy ponownie będziesz mógł zalogować się do swojego konta przejrzyj wszystkie ustawienia i preferencje konta. W ten sposób sprawdzisz czy cokolwiek zostało zmienione przez osobę, która włamała się na Twoje konto.

Cyberprzestępca uzyskał dostęp do Twoich danych?

Reaguj!

Uzyskując dostęp do Twojego konta w jakimś serwisie lub kompromitując system administratora danych, cyberprzestępca mógł zdobyć również cenne informacje na Twój temat. Takie dane jak numer PESEL, karty, dowodu czy też historia medyczna są coraz częściej głównym łupem dla internetowych złodziei. Poniżej przedstawiamy Ci kilka rzeczy, na które warto zwrócić uwagę jeśli boisz się, że takie informacje mogły dorastać się w niepowołane ręce.

- **Oświadczenia.** Jeśli podmiot odpowiedzialny za administrację Twoimi danymi osobowymi oraz wrażliwi ogłasza, że padł ofiarą ataku cybernetycznego potraktuj taką sprawę poważnie. Podczas takiego incydentu również Twoje dane mogły zostać pozyskane.
- **Wyciągi.** Podobnie jak w poprzednim punkcie zwróć uwagę na transakcje z Twoich kart płatniczych oraz kredytowych i regularnie śledź swoje wyciągi.
- **Powiadomienia i wezwania.** Ktoś karze Ci opłacić zaległości na rachunku, którego nie otworzyłeś? Dostajesz powiadomienie o konieczności spłaty raty kredytu, którego nie wziąłeś? A może dostajesz wezwanie do zapłaty za jakiś zabieg medyczny, którego nie przeszedłeś? Jeśli na któreś z powyższych pytań odpowiesz twierdząco, to bardzo możliwe, że padłeś ofiarą wycieku danych.

Jaka powinna być Twoja reakcja, jeśli zauważysz którąś z oznak?

- **Zgłoś.** Powiadom operatora usługi o zdarzeniu. W przypadku nieprawidłowości w płatnościach natychmiast skontaktuj się z bankiem oraz wystawcą karty płatniczej. Zleć również jej zastrzeżenie oraz złóż wniosek o wydanie nowej. Obecnie coraz więcej banków udostępnia również możliwość zastrzeżenia karty poprzez konto we własnym serwisie lub aplikacji.
- **Notuj.** W przypadku dokonywania jakiegokolwiek zgłoszenia dokładnie dokumentuj wszystkie informacje, które udało Ci się uzyskać. Zanotuj datę i godzinę rozmowy, poproś o imię i nazwisko konsultanta, który przyjmuje Twoje zgłoszenie. Jeśli jest ono rejestrowane w formie pisemnej zachowaj wszelką korespondencję.

Pamiętaj, że do wycieku Twoich danych może dojść w sytuacjach, które na pozór nie noszą znamion przestępstwa. Przykładowo wynajmując mieszkanie i podpisując umowę najmu podajesz drugiej osobie swoje dane osobowe tj. numer dowodu, PESEL czy adres zameldowania. Osoba taka może spreparować upoważnienie z Twoimi danymi i w ten sposób zawierać umowy w Twoim imieniu np. na podłączenie multimediów w mieszkaniu.
Nie dowiesz się o tym do momentu, aż osoba zawierająca w Twoimi imieniu umowę nie przestanie płacić rachunków. Wtedy taka sprawa zostaje przekazana do windykacji a z Tobą kontaktuje się osoba odpowiedzialna za ściągnięcie długu. Rozwiązaniem tego problemu jest niezwłoczny kontakt z firmą windykacyjną w celu wyjaśnienia sprawy (której dane uzyskasz z jej oficjalnej strony internetowej). Jeśli firma stwierdzi, że faktycznie doszło do przestępstwa koniecznie staw się na policję w celu zgłoszenia kradzieży tożsamości. Z tego względu uważaj komu i w jakich okolicznościach podajesz swoje dane osobowe.

Jak zadbać o bezpieczeństwo urządzeń mobilnych?

Bardzo atrakcyjnym łupem dla cyberprzestępcy są również wszelkiego rodzaju urządzenia mobilne. Obecnie na smartphonach czy tabletach przechowujemy „całe swoje życie". Z tego względu można wyciągnąć z nich zatrważająca ilość danych na Twój temat. Jest to z kolei niezwykle cenne dla każdego cyberprzestępcy, który chce pozyskać informacje na Twój temat. Po czym rozpoznać, że Twoje urządzenie mogło zostać zainfekowane?

- **Podejrzane strony/programy.** Twoje urządzenie kieruje Cię na strony internetowe, na które nie miałeś zamiaru wchodzi lub uruchamia nowe programy, któryś nie instalowałeś wcześniej.
- **Antywirus.** Twój program antywirusowy sygnalizuje wykrycie podejrzanego pliku. W niektórych przypadkach możesz mieć również trudności z jego zaktualizowaniem.
- **Funkcjonalność.** Cokolwiek w działaniu urządzenia budzi Twoje wątpliwości. Wszelkie anomalie w jego funkcjonalności, spadek wydajności i potoczne „wieszanie się" systemu mogą świadczyć o infekcji.
- **Niepożądane działania.** Oznakom zainfekowanego urządzenia mogą być również wykonywanie przez twoje urządzenie podejrzanych i kosztownych połączeń lub instalowanie aplikacji, na które nie wyraziłeś zgody.

Jak poradzić sobie z zainfekowanym urządzeniem? Nic prostszego!

- **Skanowanie.** Za pomocą zainstalowanego programu antywirusowego wykonaj pełne skanowanie swojego urządzenia. W przypadku odkrycia jakichkolwiek zainfekowanych plików postępuj zgodnie z instrukcjami wydawanymi przez program.

- **Reset fabryczny.** Jeśli chcesz mieć pewność, że odzyskałeś pełną kontrolę nad urządzeniem rozważ pełne zresetowanie komputera (tzw. reset fabryczny) oraz ponowną instalację systemu operacyjnego. Następnie zainstaluj najnowszą wersję wybranego przez siebie oprogramowania antywirusowego, a swoje pliki przywróć z regularnie wykonywanej (mamy nadzieję!) kopii zapasowej danych.
- **Zapobiegaj.** Jak wiadomo lepiej zapobiegać niż leczyć. Dlatego dbaj o swoje informacje i staraj się sam nie dopuszczać do ich wycieku. W tym celu możesz zainwestować w filtr anonimizujący, który możesz nakleić na ekran swojego urządzenia. Wtedy wszelkie wpisywane dane nie będą widoczne dla osób stojących obok Ciebie w transporcie publicznym, siedzących za Tobą na zajęciach na uczelni czy też kamer monitoringu.

Stosując się do naszych porad masz pewność, że poradzisz sobie w przypadku, kiedy padniesz ofiarą cyberprzestępstwa. Jednak jeśli uważasz, że incydent, który Cię dotknął jest o wiele poważniejszy i nie jesteś pewny czy jesteś w stanie samodzielnie poradzić sobie z jego następstwami zostaw tę sprawę profesjonalistom. Niestety ataki cybernetyczne stały się codziennością w XXI wieku. Padłeś ofiarą takiego zdarzenia? Przede wszystkim - zachowaj spokój, a następnie skontaktuj się z nami. Nasi specjaliści dołożą wszelkich starań w celu minimalizacji skutków ataku. Więcej szczegółów na temat działalności naszego zespołu HIRT (Hackers Incident Response Team) znajdziesz na naszej stronie. Zachęcamy Cię również do odwiedzenia naszych profili w mediach społecznościowych (Facebook oraz Twitter) , gdzie możemy podyskutować na temat bezpieczeństwa w sieci.