Co oznacza komunikat "Połączenie nie jest bezpieczne" Czyli https czy też htttp?

Kiedy Firefox, Google łączy się z zaszyfrowaną stroną (jej adres zaczyna się od "https://"), musi zweryfikować ważność certyfikatu bezpieczeństwa używanego przez odwiedzaną stronę, a także siłę zaszyfrowania, by upewnić się że twoja prywatność jest odpowiednio zabezpieczona. Jeśli certyfikat nie może zostać zweryfikowany lub też szyfrowanie nie jest wystarczająco silne, Firefox, Google przerwie połączenie ze stroną i wyświetli komunikat błędu *Połączenie nie jest bezpieczne*:

Widząc małą zieloną kłódkę opatrzoną napisem „Bezpieczna” po lewej stronie adresu internetowego, większość ludzi uważa, że strona jest bezpieczna. Podobnie jest ze słowami „Ta strona używa bezpiecznego połączenia” oraz gdy adres rozpoczyna się od „https”. Dziś coraz więcej stron wdraża HTTPS; tak naprawdę większość z nich nie ma wyjścia. W czym zatem tkwi problem? W końcu im więcej zabezpieczonych stron, tym lepiej, prawda?

Co oznaczają kłódki na pasku adresu w Google Chrome

USPL
Zadaj pytanie

Kiedy przeglądamy lub logujemy się na konkretne strony internetowe, zawsze musimy zwracać uwagę na poziom bezpieczeństwa danej strony. Symbolem, który może dostarczyć nam konkretnych informacji jest symbol kłódki znajdujący się po lewej stronie paska adresowego.

W tej poradzie wyjaśnimy, co oznaczają konkretne symbole, które widoczne są w pasku adresu przeglądarki Google Chrome.

Google Chrome - znaczenie kłódek na pasku adresu

Zielona kłódka - oznacza, że połączenie z daną stroną jest bezpieczne, strona jest bowiem wyposażona w sprawdzony i ważny certyfikat. Jeśli dodatkowo, obok zielonej kłódki, pojawi się element **https**, oznacza to, że strona jest szyfrowana.

Tego typu oznaczenia powinny pojawić się na stronach, które wymagają podania tzw. danych wrażliwych, czyli loginu i hasła dostępu. Przykładem mogą być na przykład bankowość internetowa czy usługa Dysk Google.

Żółty symbol wykrzyknika: oznacza, że dana strona nie udostępniła certyfikatu przeglądarce. Najczęściej dzieje się tak w przypadku stron zawierających element **http**, które nie korzystają z certyfikatów SSL.

W przypadku stron, na których nie ma konieczności podawania loginu czy hasła, jest to bezpieczne rozwiązanie. Jeśli jednak żółty symbol wyświetla się na stronie, na której należy wprowadzić jakiekolwiek dane, zastanów się dwa razy, zanim podejmiesz taki krok!

Czerwona kłódka ze znakiem krzyżyka: informuje o błędach wykrytych w certyfikacie strony. W przypadku takiego komunikatu należy zachować szczególną ostrożność i nie wprowadzać żadnych danych. Najprawdopodobniej bowiem ktoś podszywa się pod daną witrynę, aby przechwycić cenne informacje.

Klikając w symbol kłódki w przeglądarce Google zyskujesz dostęp do dodatkowych informacji na temat odwiedzanej witryny. Jeśli klikniesz w zakładkę **Połączenie**, oprócz symboli, które umówiliśmy powyżej może pojawić się również ikona **kłódki na szarym tle z żółtym trójkątem**. Jej wyświetlenie oznacza, że na stronie znajdują się niezaszyfrowane elementy, które mogą stanowić zagrożenie, jeśli zechcemy wpisać jakiekolwiek dane. Należy więc zachować czujność.

Poza informacjami o poziomie bezpieczeństwa, w zakładce **Połączenia** znajduje się również informacja o tym, czy i kiedy dana strona była przez nas odwiedzana.


HTTP
SSL
HTTPS


https://


https://


HTTPS

Bezpieczne połączenie nie gwarantuje, ze strona nie jest szkodliwa

Zielona kłódka oznacza, że strona otrzymała certyfikat, do którego wygenerowano klucze kryptograficzne. Wówczas strona szyfruje informacje, które są przesyłane podczas komunikacji z Tobą, a jest to oznaczone symbolem HTTPS widocznym na początku jej adresu, w którym ostatnia litera — „S” — oznacza „Secure”, czyli „Bezpieczna”.

Oczywiście szyfrowanie przesyłanych danych jest bardzo potrzebne: informacje wymieniane między przeglądarką a stroną nie są dostępne dla podmiotów zewnętrznych — dostawców usług internetowych, administratorów sieci, osób obcych itp. Umożliwia ono wprowadzanie haseł lub szczegółów związanych z kartą kredytową bez możliwości ich podejrzenia przez kogoś postronnego.

Problem w tym, że zielona kłódka oraz otrzymany certyfikat nic nie mówią o samej stronie. Wobec tego strona phishingowa także może uzyskać certyfikat i szyfrować cały ruch, który odbywa się między nią a użytkownikiem.

Mówiąc wprost, wszystkie zielone kłódki oznaczają, że nikt inny nie ma dostępu do wprowadzanych danych. Jeśli jednak strona jest fałszywa, hasła mogą zostać skradzione.

Korzystają z tego faktu phisherzy: według informacji opublikowanych na blogu PhishLabs obecnie za pośrednictwem stron HTTPS przeprowadzana jest jedna czwarta wszystkich ataków phishingowych (dwa lata temu było ich mniej niż 1%). Co więcej, ponad 80 procent użytkowników wierzy, że sam fakt istnienia tej małej zielonej kłódki oraz słowa „Bezpieczna” wyświetlanego obok adresu internetowego oznacza, że strona nie jest szkodliwa, przez co ludzie ci bez namysłu wprowadzają swoje dane.

A co w sytuacji, gdy kłódka ma inny kolor niż zielony?

Jeśli w pasku adresu nie ma kłódki, strona nie wykorzystuje szyfrowania i wymienia informacje z przeglądarką przy użyciu standardowego protokołu HTTP. Przeglądarka Google Chrome zaczęła oznaczać takie strony jako niebezpieczne. Choć mogą one być czyste jak łza, nie szyfrują ruchu między użytkownikiem a serwerem. Większość właścicieli stron nie chce, aby Google oznaczał je jako niebezpieczne, więc coraz więcej z nich decyduje się na zastosowanie opcji HTTPS. W każdym przypadku wprowadzanie wrażliwych danych na stronie HTTP nie jest dobrym pomysłem, bo każdy może je podejrzeć.

Może się też zdarzyć, że ikona kłódki jest przekreślona na czerwono, a kolorem tym jest oznaczony również skrót HTTPS. Oznacza to, że strona ma certyfikat, ale nie został on zweryfikowany lub jest przestarzały: w efekcie połączenie między użytkownikiem a serwerem jest szyfrowane, lecz nie ma gwarancji, że domena należy do firmy wskazanej na stronie. Jest to najbardziej podejrzany scenariusz; zazwyczaj takie certyfikaty są używane jedynie do celów testowych.

Jeśli certyfikat wygaśnie i właściciel nie zadba o jego odnowienie, przeglądarki będą oznaczać stronę jako niebezpieczną, jednak w bardziej stanowczy sposób — poprzez wyświetlanie czerwonej kłódki. W takich przypadkach lepiej unikać takich stron — nie wspominając o wprowadzaniu na nich jakichś danych osobistych.

Jak nie paść ofiarą oszustwa

Podsumowując, obecność certyfikatu i zielona kłódka oznaczają tylko tyle, że dane przesyłane między użytkownikiem a serwerem są szyfrowane, a certyfikat został wydany przez zaufany organ certyfikujący. Jednak nie zapobiega to sytuacji, w której strona HTTPS jest szkodliwa, a fakt ten jest najczęściej wykorzystywany przez oszustów phishingowych.

Dlatego zawsze należy zachować czujność — bez względu na to, jak bezpieczna wydaje się strona na pierwszy rzut oka.

- Nigdy nie wprowadzaj loginów, haseł, danych bankowych ani żadnych innych informacji osobistych na stronie, dopóki nie upewnisz się, że jest autentyczna. W tym celu zawsze dokładnie sprawdzaj nazwę domeny; nazwa fałszywej strony może się różnić nawet tylko jednym znakiem. Upewnij się, że łącza nie są szkodliwe, zanim je klikniesz.
- Zawsze zatrzymaj się na chwilkę i zastanów się, co konkretna strona oferuje, czy wygląda podejrzanie i czy naprawdę musisz się na niej rejestrować.
- Upewnij się, że Twoje urządzenie jest dobrze chronione: Kaspersky Internet Security sprawdza adresy internetowe w obszernej bazie stron phishingowych, a także wykrywa oszustwa bez względu na to, jak „bezpiecznie" ona wygląda.

Do zabezpieczania sieci bezprzewodowych najlepiej mogą zachęcić praktyczne przykłady tego, co cyberwłamywacze są w stanie bez specjalnego wysiłku przechwycić z niezaszyfrowanej sieci Wi-Fi. Jest to też sposób, żeby pokazać, kiedy szyfrowanie jest potrzebne.

Przyjrzymy się kilku różnym usługom i rodzajom komunikacji sieciowej, które są podatne na przechwytywanie i łatwo je odczytać. Wyjaśnimy również, jak zabezpieczyć te usługi. Omawiane przykłady dotyczą przede wszystkim korzystania z niezabezpieczonych punktów dostępowych, prywatnych i publicznych. Mimo że w przypadku firmowych sieci występują te same podatności, włączenie szyfrowania WPA lub WPA2 ukrywa całą komunikację przed potencjalnym włamywaczem. Dlatego upewnij się, że Twoja sieć Wi-Fi używa szyfrowania.

Odwiedzane strony internetowe
Najpierw przyjrzymy się najprostszej usłudze – połączeniom HTTP, czyli komunikacji pomiędzy przeglądarką internetową, a serwerem WWW. Podsłuchiwacz może podejrzeć, jakie strony WWW odwiedzasz – adresy IP są wyszczególnione w przesyłanych pakietów. Aczkolwiek, metoda ich wydobywania jest dość toporna. Sniffer, np. bezpłatny Wireshark, przechwytuje adresy razem z kodem HTML, PHP i innymi elementami strony WWW.

Jeśli włamywacz chce ułatwić sobie zadanie, możesz wykorzystać bardziej zaawansowany sniffer, który przechwytuje pakiety oraz interpretuje przechwycone pliki i kod. W ten sposób można nie tylko sprawdzić adres strony, ale także od razu ją podejrzeć. Zwróć uwagę, że włamywacz widzi te same dane, co ty. Może je także zapisać, np. wybrane dokumenty czy obrazy.

Natomiast w przypadku połączeń zabezpieczonych szyfrowaniem dane są zakodowane i trudne do odczytania. Jeśli korzystasz z banku internetowego czy kupujesz coś w e-sklepie, płacąc kartą kredytową, połączenie między komputerem, a serwerem WWW jest z reguły zaszyfrowane niezależnie od ustawień Twojej sieci. W przypadku takich serwisów internetowych stosuje się protokół SSL, którego działanie

rozpoznasz po adresie URL – będzie się on rozpoczynał od HTTPS, a nie od HTTP. Ponadto przeglądarka wyświetli symbol zamkniętej kłódki, informując, że połączenie jest zabezpieczone.

Nie musisz się przejmować niezabezpieczonymi stronami WWW, jeśli Twoja sieć Wi-Fi ma włączone szyfrowanie WPA lub WP2. Jednakże w sieciach publicznych, jeśli chcesz zabezpieczać połączenia z niechronionymi stronami, należy używać sieci VPN. W Internecie działają serwisy oferujące szyfrowane połączenia VPN, zarówno płatnie, jak i bezpłatnie. Dzięki ich usługom możesz czuć się bezpiecznie, korzystając z publicznego, niezabezpieczonego hotspotu.

Przesyłanie plików
Jeśli w niezabezpieczonej sieci przesyłasz pliki między komputerami czy pobierasz pliki z Internetu, są one podatne na przechwycenie. Włamywacz może przejrzeć przechwycone pakiety i z łatwością odczytać zawartość plików tekstowych. A jeśli dysponuje bardziej wyrafinowanym snifferem, będzie w stanie otworzyć również inne pliki – dokumenty, skompresowane archiwa, obrazy – i zapisać je w swoim komputerze.

W tym przypadku użycie szyfrowania WPA lub WPA2 również rozwiązuje problem. W sieci niezabezpieczonej czy w sieci publicznej, nie należy udostępniać plików. Najlepiej, jeśli wyłączysz usługi udostępniania plików i drukarek we właściwościach połączeń sieciowych w Windows XP, Vista czy Windows 7.

Dane dostępowe do kont pocztowych oraz wiadomości e-mail
Szczególnym przypadkiem stron internetowych jest tzw. webmail, czyli dostęp do konta pocztowego przez przeglądarkę WWW. Wspomnieliśmy już o zagrożeniach związanych z niezabezpieczonymi stronami. W kontekście dostępu do konta pocztowego bez szyfrowania SSL oznacza to, że wiadomości są narażone na przechwycenie i odczytanie przez włamywacza. Niektóre serwisy zawsze zapewniają szyfrowany dostęp, ale są też takie, w których szyfrowanie jest opcjonalne lub w ogóle jest niedostępne. Przykładowo, Gmail w domyślnej konfiguracji nie szyfruje transmisji.

Aby sprawdzić, czy Twój dostawca poczty oferuje szyfrowanie transmisji, w adresie URL dodaj literkę S po ciągu znaków HTTP. Przykładowo, zamiast http://mail.google.com, wpisz https://mail.google.com. Jeśli używasz klienta pocztowego, np. Outlooka, zabezpieczenie komunikacji POP3 jest trochę bardziej skomplikowane.

Stosując szyfrowanie WPA/WPA2 w swojej sieci Wi-Fi, zapobiegniesz przechwyceniu wiadomości przez niepowołane osoby. Jeśli nie możesz lub nie chcesz zabezpieczać komunikacji z serwerem pocztowym, możesz korzystać z połączeń VPN.

Dane dostępowe do serwera FTP, transfer plików
Jeśli w niezabezpieczonej sieci przesyłasz pliki pomiędzy serwerem FTP, a swoim komputer, sniffer może je przechwycić. Poza tym, podobnie jak w przypadku poczty elektronicznej, dane dostępowe są przesyłane w postaci tekstowej, więc są bardzo łatwe do odczytania.

Niestety, nie ma możliwości zaszyfrowania samych połączeń FTP, natomiast można włączyć szyfrowanie całej komunikacji w sieci Wi-Fi. W sieciach publicznych w ogóle nie należy korzystać z FTP dopóki nie skonfiguruje się połączenia VPN. Jeśli jesteś administratorem serwera, możesz zabezpieczyć komunikację, uruchamiając protokół SFTP.

Komunikatory internetowe
Większość komunikatorów internetowych i czatów, włączając w to Gadu-Gadu i IRC, wysyła wiadomości czystym tekstem. Dlatego, jeśli korzystasz z sieci publicznej, włamywacz może z łatwością śledzić Twoje konwersacje. Ponownie, aby zabezpieczyć taką komunikację, należy korzystać z połączeń VPN.

Dane dostępowe telnetu
Trzeba pamiętać o telnecie, który również przesyła dane dostępowe prostym tekstem. Nie korzystaj z niego w sieciach publicznych, chyba że masz połączenie VPN. Zamiast telnetu warto używać bezpiecznego protokołu SSH.

Zabezpieczanie
Opisaliśmy kilka usług sieciowych, które są narażone na podsłuchiwanie w niezabezpieczonych sieciach Wi-Fi. Każdy będący w zasięgu takiej sieci może sprawdzić, jakie strony WWW odwiedzasz, odczytać treść wiadomość e-mail czy dane dostępowe do serwera FTP. Aby temu zaradzić:

- Włącz szyfrowanie WPA lub WPA2 w twojej sieci. W ten sposób uniemożliwisz podsłuchiwanie odbywającej się w niej komunikacji.
- Niezależnie od tego zabezpieczaj same usługi sieciowe. Używaj szyfrowania w przypadku usług, które oferują taką możliwość, np. poczta elektroniczna. Używaj alternatyw, np. SSH zamiast telnetu, a pliki przesyłaj przez bezpieczną pocztę a nie serwer FTP. Korzystaj z usług internetowych szyfrujących połączenia protokołem SSL (HTTPS).
- W sieciach publicznych korzystaj z połączeń VPN. Szyfruje one całą komunikację, chroniąc ją przed odczytaniem przez włamywacza. Serwis AnchorFree www.anchorfree.com oferuje bezpłatną usługę SSL VPN.
- Nie używaj jednego hasła dla wszystkich usług. Jeśli włamywacz pozna hasło do jednej usług, nie należy mu ułatwiać zadania I uniemożliwić dostęp do pozostałych usług. Są narzędzia, które umożliwiają bezpieczne przechowywanie haseł, żeby użytkownik nie musiał ich wszystkich pamiętać.