



STÓJ | POMYŚL | POŁĄCZ

RANSOMWARE: FAKTY I DOBRE PRAKTYKI

Postęp techniczny oprócz niewątpliwych zalet wiąże się także z pewnymi niebezpieczeństwami. Jednym z nich jest złośliwe oprogramowanie ransomware. Tak jak w codziennym życiu dbamy o zdrowie, przestrzegając zasad higieny, podobnie w cyfrowym świecie warto znać i stosować zasady sprzyjające naszemu bezpieczeństwu.

CZYM JEST RANSOMWARE?

Ransomware to szkodliwe oprogramowanie, które odbiera Ci dostęp do Twoich plików poprzez ich zaszyfrowanie. Być może zauważyłeś, że w nazwie znajduje się angielskie słowo *ransom*, oznaczające *okup*. Po przeprowadzonym ataku, w zamian za przywrócenie dostępu do danych, przestępcy żądają zapłaty okupu, określonej kwoty pieniędzy. Chcąc zainfekować komputer swojej ofiary, atakujący umieszczają złośliwy odnośnik lub załącznik w wiarygodnej, lecz fałszywej wiadomości e-mail. Zaszyfrowane zostają dokumenty, fotografie, pliki projektowe, wrażliwe dane przedsiębiorstwa, etc. Potencjalnym celem ataku może stać się zarówno firma, jak i osoba prywatna.

CO MOŻESZ ZROBIĆ?

Każdy z nas może przyczynić się do poprawy bezpieczeństwa w Internecie. Poniżej podajemy kilka zaleceń kampanii STÓJ. POMYŚL. POŁĄCZ. przygotowanych w celu lepszej ochrony przed ransomware i innymi zagrożeniami w sieci.



Zadbaj o aktualizacje: Pamiętaj by regularnie aktualizować urządzenia podłączone do Internetu. System operacyjny na komputerze i smartfonie, oprogramowanie antywirusowe, czy aplikacje z których korzystasz - powinny być uruchamiane w najnowszej dostępnej wersji.



Dwuskładnikowe uwierzytelnianie: Coraz więcej serwisów, wśród nich bankowość internetowa, poczta e-mail, portale społecznościowe, oferuje funkcję dwuskładnikowego uwierzytelniania. Włącz ją i bądź spokojniejszy o swoje bezpieczeństwo. Od teraz weryfikacja Twojej tożsamości poza podaniem loginu i hasła będzie wymagała spełnienia dodatkowego warunku, np. podania kodu SMS przesyłanego na Twój telefon.



Twórz kopie zapasowe: Zabezpiecz efekty swojej pracy, muzykę, zdjęcia, cenne dokumenty. Regularnie wykonuj kopie zapasowe i przechowuj je w bezpiecznym miejscu.



Stwórz mocne hasło: Dobre hasło składa się z przynajmniej 12 znaków. Skup się na pozytywnych zdaniach lub zwrotach o których lubisz myśleć i które łatwo zapamiętasz (np. „Kocham miasto muzyki”). Na wielu stronach internetowych, możesz przy wprowadzeniu hasła użyć spacji.



Bądź świadomym użytkownikiem: Odnośniki i załączniki w wiadomościach e-mail, spreparowane posty w mediach społecznościowych, a także reklamy - to częste metody używane przez przestępców w celu kradzieży danych. W momencie, gdy wydają Ci się podejrzane, po prostu je zignoruj. Nawet jeżeli źródło wygląda na zaufane.



Skanuj nośniki wymienne: Nie podłączaj do komputera urządzeń, których pochodzenie nie jest Ci znane. Pendrive'y, dyski zewnętrzne i inne nośniki danych mogą być niebezpieczne (zainfekowane przez szkodliwe oprogramowanie). Zanim otworzysz ich zawartość, skorzystaj ze skanera antywirusowego.