Zasady bezpiecznego korzystania z Internetu

Na bieżąco aktualizuj swój komputer

Wykorzystywanie luk w systemach operacyjnych, przeglądarkach, aplikacjach na komputerze stacjonarnym, urządzeniach moblinych to jedna z częstszych metod stosowanych przez cyberprzestępców. W samym 2020 zostało wykrytych aż 18 100 podatności (liczba ta jest znacznie większa niż w poprzednich latach). Warto więc korzystać z automatycznych aktualizacji.

Używaj silnych haseł

Hasła są tak naprawdę kluczami do naszych wrażliwych danych. Mamy coraz więcej kont i profili przez co korzystamy z prostych/ "słabych" ciągów znaków i nie uwierzytelniamy się wieloskładnikowo. To niestety ogromna możliwość i szansa dla cyberprzestępców. Wystarczy skorzystać ze specjalnych narzędzi łamiących słabe, jednostronne szyfrowanie, testować powszechnie używane warianty, wypróbować złamane hasła na innych kontach. Dobrą praktyką jest korzystanie z menadżera by tworzyć i zapamiętywać unikalne hasła.

Nie korzystaj z publicznej sieci Wi-Fi

Ogólnodostępne i darmowe Wi-Fi w przestrzeni publicznej to już standard. Trzeba mieć świadomość, że z tej samej sieci mogą korzystać także hakerzy. W przypadku, gdy nie masz możliwości uzyskania innego połączenia nie loguj się do kont z wrażliwymi danymi.

Sprawdzaj linki i nie klikaj bezmyślnie

Phishing jest jednym z najbardziej popularnych zagrożeń. Nie wykonuj pochopnych ruchów pod presją czasu. Hakerzy korzystają z metod socjotechniki i będą próbowali zmusić Cię do kliknięcia w zainfekowany link.

Nie podawaj danych przez telefon

E-maile i sms-y phisingowe to równie częste zjawisko. Wykorzystując socjotechnikę cyberprzestępca próbuje nakłonić potencjalną ofiarę by podała mu wrażliwe dane osobowe. Podobnym atakiem jest vishing (phishing głosowy), czyli podszywanie się np. pod pracownika banku, wiarygodną instytucję/korzystanie z podobnych numerów telefonu. W przypadku takiego kontaktu należy zapytać rozmówcę kim jest i kogo reprezentuje, następnie skontaktować się z taką osobą za pomocą oficjalnie udostępnionych kanałów komunikacji. W ten sposób zweryfikujesz przekazane informacje i dzwoniącego. Pamiętaj! Podczas weryfikowania nie używaj numerów dzwoniącego i nie podawaj żadnych danych.

Zabezpieczaj wszystkie typy urządzeń – bezpieczeństwo w Internecie

Oprogramowania chroniące np. przed malwarem powinny być zainstalowane na wszystkich urządzeniach, które mają dostęp do sieci. Warto zaznaczyć by korzystać z rozwiązań renomowanych producentów i zadbać nie tylko o komputer stacjonary, ale także o wszystkie urządzenia mobilne (telefony, tablety itd.). Bezpieczne korzystanie z Internetu to podstawa!

Nie korzystaj z niezabezpieczonych witryn

Czy wiesz dlaczego kłódka w pasku przeglądarki jest istotna? Oznacza to, że odwiedzona przez Ciebie witryna ma poprawny i ważny certyfikat. Informuje także o tym, że dana strona prawdopodobnie zapobiega przechwytywaniu danych (chociaż nie daje całkowitej gwarancji bezpieczeństwa, wiele stron phishingowych używa HTTPS).

Odróżniaj życie prywatne od zawodowego

Przez pandemię coraz cześciej korzystamy z możliwości pracy zdalnej lub hybrydowej. Niebezpiecznym zjawiskiem stało się używanie służbowych adresów e-mailowych do rejestracji kont w celu zakupów konsumenckich. Ryzyko pojawia się także w momencie używania niezabezpieczonych urządzeń prywatnych.

Zadbaj o kopie zapasowe

Ofiarami ataków typu ransomware mogą stać się tak naprawdę wszyscy, osoby prywatne, firmy, instytucje. Każdy z nas narażony jest na utratę ważnych dokumentów. Aby nie musieć negocjować z cyberprzestępcami musimy pamiętać o wykonywaniu kopii zapasowych. Warto korzystać z co najmniej dwóch, różnych nośników i przechowywać je w innych lokalizacjach.

Zmień domyślne hasła w urządzeniach inteligentnych

Inteligentne kamery, telewizory, asystenci – jedna trzecia domów europejskich jest wyposażona w urządzenia typu smart city i smart home. Wszystko co jest podłączone do sieci jest atrakcyjnym celem dla oszustów. Urządzenia mogą zostać przejęte, zamienione w botnety do przeprowadzania ataków lub stać się bramą dla pozyskania pozostałych inteligentnych gadżetów. Co należy zrobić? Pamiętaj w szczególności o zmianie domyślnych haseł, wybierz znanego producenta, ktory przeprowadza badania pod kątem luk i przyszłościowych napraw.

Podsumowanie

Największym wyzwaniem jest to, że zagrożenia ciągle i szybko ewoluują, dlatego tak bardzo ważne jest by pamiętać o podstawowych zasadach i zadbać o swoje bezpieczeństwo już teraz, inwestując w odpowiednie rozwiązania.

Źródło:

https://www.netcomplex.pl/blog/jak-byc-bezpiecznym-w-sieci-zasady-cyberbezpieczenstwa