Dzień Bezpiecznego Internetu: sprawdź, co możesz zrobić, by uniknąć zagrożeń

Dzień Bezpiecznego Internetu, to świetna okazja, by pochylić się nad tytułowym bezpieczeństwem w sieci. Choć wszystkie zasady związane ze zdrowym rozsądkiem czy też oprogramowaniem zabezpieczającym powinny być bliskie każdemu internaucie na co dzień, dzisiaj szczególnie warto zwrócić na nie uwagę i być może zmienić swoje dotychczasowe, niekoniecznie najlepsze nawyki.

Warto bowiem pamiętać, że *bezpieczeństwa w sieci* nie zagwarantuje tylko omijanie podejrzanych witryn i korzystanie ze skanera antywirusowego podczas pobierania plików. Oszuści są gotowi wykorzystać każdy błąd użytkownika i luki systemów, aby wejść w posiadanie cudzych danych i koniec końców wykorzystać je do wzbogacenia się. Poniżej znajduje się zestawienie kilku najważniejszych poradników, które pozwolą każdemu w prosty sposób zadbać o swoje, w tym przypadku szeroko rozumiane, bezpieczeństwo w sieci.

Sprawdź, czy twoje dane nie zostały wykradzione

Dość przewrotnie, zacząć warto od sprawdzenia, czy dane już teraz nie są dostępne dla oszustów. Do sieci mogły trafić w wyniku jednego z wcześniejszych ataków na bazy, które wcale nie należą do rzadkości. Zamiast samodzielnie zmieniać nazwy użytkowników i hasła do wszystkich serwisów, z których korzysta dana osoba, dla ułatwienia można skorzystać z witryn, które same podpowiedzą, czy wskazane dane nie zostały już wcześniej ujawnione. To pomoże zdecydować, czy na tym etapie jest potrzeba zmiany haseł.

Narzędziem, które w tym przypadku proponujemy jest witryna Have I Been Pwnd. To swego rodzaju baza danych z wszystkich znanych, dotychczasowych wycieków, które można w łatwy przeszukiwać, a w efekcie porównywać ze swoimi danymi. Po wejściu na stronę należy wprowadzić swój adres e-mail aby sprawdzić, czy wykorzystujące go konta są jeszcze bezpieczne. Jako ciekawostkę warto dodać, że z tego samego mechanizmu korzysta Firefox Monitor, który wbrew sugestywnej nazwie dostępny jest dla użytkowników dowolnej przeglądarki.

Zabezpiecz dostęp do kont uwierzytelnianiem dwuskładnikowym

Aby w przyszłości zapewnić sobie większe bezpieczeństwo podczas logowania do różnych serwisów, warto skorzystać z uwierzytelniania dwuskładnikowego. To metoda logowania dostępna na wielu stronach, w tym w serwisie Facebook, Instagram, Twitter oraz w szeregu aplikacji Google'a, w tym Gmailu. W praktyce chodzi o rozszerzenie etapu logowania o konieczność podania jednorazowego hasła generowanego przez aplikację lub wysyłanego do użytkownika SMS-em.

Dzięki takiemu podejściu, nawet jeśli atakujący wejdą w posiadanie loginu i hasła do konta, i tak nie będą ich mogli wykorzystać do zalogowania, o ile nie zdobędą od użytkownika także smartfona, na którym pojawi się właściwe jednorazowe hasło. Osoby ceniące prywatność powinny więc zainteresować się tym rozwiązaniem i nie obawiać ewentualnego zablokowania konta – najczęściej podczas konfiguracji uwierzytelniania dwuskładnikowego można pobrać zapasowe kody, które pozwolą dostać się do konta w awaryjnych sytuacjach (na przykład, gdy smartfon zostanie zniszczony).

Naucz się rozpoznawać phishing

Jedną z częściej stosowanych form ataku jest phishing, czyli w praktyce poleganie na łatwowierności i nieuwadze użytkownika. Oszuści rozsyłają do swoich potencjalnych ofiar wiadomości e-mail lub SMS-y, w których umieszczają zainfekowane załączniki lub linki do sfabrykowanych stron, najczęściej związanych z płatnościami. Jeśli odbiorca nie zorientuje się, że otrzymana wiadomość jest fałszywa, łatwo może trafić na podrobioną wersję bankowości internetowej, do której próbując się zalogować – przekaże dane oszustom.

Warto więc być wyczulonym na tego typu ataki, które skutecznie działają na odbiorców i usypiają ich czujność. Swoją umiejętność rozpoznawania fałszywych wiadomości można także od niedawna sprawdzać w interesującym teście, który przygotowali pracownicy z Google. Zadaniem użytkownika jest rozpoznanie wszystkich sfabrykowanych e-maili.

Zadbaj o prywatność w smartfonie z Androidem

Bezpieczeństwo w sieci ma oczywiście znaczenie także podczas korzystania ze smartfona. W przypadku systemu Android warto więc rozumieć znaczenie uprawnień i w razie potrzeby świadomie korzystać z dodatkowych sposobów zabezpieczania prywatności. Skorzystać warto z bezpiecznej klawiatury, poczty, komunikatorów i wreszcie przeglądarki.

Aby zapewnić sobie bezpieczeństwo, nie trzeba być w tym przypadku ekspertem. W praktyce wystarczy zrozumienie kilku pojęć, zajrzenie do systemowych ustawień i wreszcie instalacja prostych w obsłudze aplikacji.

Nie daj się śledzić

Jednym z najbardziej rozbudowanych zagadnień związanych z bezpieczeństwem w Internecie jest temat podsłuchiwania i śledzenia aktywności – także tych osób, które po prostu przeglądają strony i pozornie nie wykonują działań, które mogłyby być atrakcyjne dla atakujących. Istnieje wiele sposobów, aby sobie z tym poradzić, począwszy od stosowania

blokerów niechcianych treści i skryptów śledzących, na korzystaniu z bezpiecznych i szyfrowanych komunikatorów kończąc.

Zabezpiecz smartfon dziecka

Jeśli twoje dziecko ma już własny smartfon lub czasem korzysta z twojego urządzenia, zdecydowanie warto pomyśleć nad dodatkowymi zabezpieczeniami. Z jednej strony pozwolą one ochronić cenne dane z urządzenia rodzica przed niepowołanym dostępem, a z drugiej – pociechę przed skorzystaniem z aplikacji, które mogłyby być dla niej nieodpowiednie i na przykład wyświetlać niebezpieczne treści z sieci.

To rodzic decyduje, jakie programy będą w nim dostępne, a całość zabezpiecza PIN-em.

W praktyce dzięki właściwym aplikacjom można stworzyć w smartfonie izolowane środowisko, które pozwoli dziecku uruchomić tylko te aplikacje, które wcześniej wskazał rodzic. W ten sposób da się więc na przykład zablokować dostęp do przeglądarki (za pomocą której dziecko mogłoby dostać się na strony o nieodpowiedniej treści) i udostępnić tylko wybrane gry.

Rób zakupy z rozwagą

O bezpieczeństwie warto szczególnie pamiętać także podczas internetowych zakupów. Dla oszustów to właśnie etap płatności za zamówienie jest dobrą okazją do posunięcia kupującemu fałszywej strony po kliknięciu w podejrzany link. Chociaż najczęściej takie ataki mają miejsce w okresie przedświątecznym, istnieje szereg wskazówek, które warto mieć na uwadze bez względu na porę zakupów.

Specjaliści sugerują, że w tym przypadku wystarczy przestrzegać 7 głównych zasad, mając na uwadze między innymi korzystanie ze zaktualizowanego oprogramowania zabezpieczającego. Jednym z mniej szablonowych sposobów ochrony może być natomiast wybieranie wyłącznie przesyłek za pobraniem – eksperci sugerują, że to w praktyce jedyny skuteczny sposób, który pozwala uniknąć zagrożenia na etapie płatności za zamówienie za pośrednictwem elektronicznej bankowości.

Źródło: dobreprogramy.pl