Kraków, 27 kwietnia 2017 r.

Zostań Internetowym ninja – zabezpiecz się przed atakami hakerów

**Powszechny dostęp do Internetu na coraz większej ilości urządzeń daje nam niesamowite możliwości komunikacji, pracy i rozrywki. Jednak w świecie Internetu za wygodę często płacimy bezpieczeństwem. Cyberprzestępcy szukają naszych błędów, wykorzystują chwile nieuwagi lub sami prowokują niebezpieczne zachowania. W jaki sposób najlepiej się przed nimi bronić?**

Podstawowym narzędziem, jakiego używamy do ochrony komputerów, są programy antywirusowe. Jednak, żeby zagwarantować pełną ochronę, należy podjąć dodatkowe działania. W kwestii bezpieczeństwa najważniejsze jest zachowanie ostrożności i zdrowego rozsądku. Usunięcie wirusów i innych szkodliwych aplikacji z urządzenia jest zawsze trudniejsze, niż zabezpieczenie się przed nimi. O szkodach, jakie urządzeniom wyrządza złośliwe oprogramowanie, dużo wiedzą osoby, które je naprawiają. Z tego względu eksperci serwisu GoRepair przygotowali kilka zasad, które pomogą ochronić urządzenie.

**Unikaj podejrzanych reklam, stron i linków**

Niesamowite nagłówki, atrakcyjne reklamy, powiadomienia o wygranej - potencjalne niebezpieczeństwa czyhają na nieuważnych internautów niemal wszędzie. Phishing, czyli podszywanie się pod inne osoby lub instytucje w celu wyłudzenia danych osobowych czy haseł to jedna z najpopularniejszych metod internetowych oszustów. Przestępcy tworzą imitacje wiadomości od firm telekomunikacyjnych czy kurierskich i wysyłają e-maile łudząco podobne do tych prawdziwych. Wystarczy kliknąć zamieszczony w nich link lub pobrać załącznik, aby stać się ofiarą złośliwego oprogramowania.

Każdemu z nas zdarzyło się zobaczyć na ekranie przeglądarki wyskakujące imitacje reklam i podejrzane powiadomienia. Zdarza się to zarówno na komputerach, jak i smartfonach. Wszystkie wiadomości o krytycznych błędach, wykrytych wirusach czy koniecznych aktualizacjach to kłamstwa. Czasami nawet kliknięcie przycisku „zamknij” lub „odrzuć” daje hakerowi możliwość przekierowania użytkownika na inną stronę lub instalację złośliwego oprogramowania. Niebezpieczne linki możemy znaleźć również w pojawiających się w mediach społecznościowych sensacyjnych nagłówkach, a nawet prywatnych wiadomościach.

Obrona przed tymi zagrożeniami jest stosunkowo prosta. Przede wszystkim, należy zwracać uwagę na adresy stron, które wymagają podania hasła. Najbezpieczniejsze są te, obok których widnieje ikona kłódki, czyli korzystające z szyfrowanego protokołu HTTPS. Jeżeli witryna o adresie „facebokk.com” poprosi o wpisanie danych logowania, możemy mieć pewność, że mamy do czynienia z oszustwem. Najprostszą radą w tym przypadku jest nieklikanie i nieotwieranie treści, do których nie mamy pełnego zaufania.

Najpopularniejsze przeglądarki wyposażone są w narzędzia ostrzegające użytkowników o stronach, które mogą wyrządzić szkodę. Większość programów antywirusowych posiada również swoje wtyczki do przeglądarek, które dodatkowo zabezpieczają przeglądanie sieci.

**Zaktualizuj oprogramowanie**

Pojawiające się systematycznie na ekranie komputera powiadomienia o konieczności zaktualizowania oprogramowania są irytujące dla nas wszystkich. Ale w kwestii bezpieczeństwa mają one ogromne znaczenie. Aktualizacje programów, przeglądarek czy systemu operacyjnego często dotyczą ochrony przed atakami. Są one szczególnie ważne, kiedy w danym oprogramowaniu została wykryta luka w zabezpieczeniach. Każde takie zdarzenie to idealna okazja dla hakerów na przejęcie kontroli i zainfekowanie kolejnych urządzeń. Najważniejsze jest oczywiście posiadanie najnowszych wersji programów antywirusowych - to one bezpośrednio zabezpieczają sprzęt. *„Złośliwe oprogramowanie może prowadzić nie tylko do utraty danych, ale też do awarii oprogramowania i sprzętu. W takich przypadkach warto skorzystać z pomocy specjalistów, którzy pomogą przywrócić urządzenie do poprawnego działania”* - dodaje Piotr Pachota z serwisu GoRepair.

**Stosuj mądre hasła**

Konto bankowe, Facebook, Twitter, skrzynka mailowa, YouTube, Snapchat, Spotify, Netflix. Lista portali i usług, do których musimy zapamiętać hasła, jest długa. Dane logowania pełnią taką samą funkcję jak klucz do drzwi naszego mieszkania. Niestety, wielu internautów ignoruje ten fakt. Zgodnie z rankingiem keepersecurity.com z 2016 roku, najpopularniejszym hasłem w usługach i portalach było „123456”. Korzystało z niego aż 17% użytkowników. Kolejne pozycje można równie łatwo zgadnąć – „123456789”, „qwerty”, „12345678”, „111111”. Nie gwarantują one żadnego bezpieczeństwa, a mimo to z 25 najpopularniejszych haseł korzysta ponad połowa internautów. Należy zwracać uwagę nie tylko na to, żeby dane do logowania były trudne do odgadnięcia, ale również, żeby były różne w poszczególnych usługach czy portalach. Utrudni to zadanie cyberprzestępcom i pomoże ochronić nasze cenne dane.

**Uważaj na otwarte sieci Wi-Fi**

Otwarte sieci Wi-Fi i niezabezpieczone routery są wyjątkowo łatwym celem dla hakerów. Według raportu firmy Fortinet z 2016 roku, urządzenia tego typu zostały zaatakowane aż 25 miliardów razy! Za rekordowym wynikiem stoi luka w zabezpieczeniach urządzeń jednego z producentów. Przez sieć bezprzewodową można w stosunkowo prosty sposób uzyskać dostęp do danych przesyłanych przez użytkowników. Hakerzy mogą nawet przejąć kontrolę nad urządzeniem. Bezpieczeństwo surfowania w Internecie zapewniają tylko zamknięte i zabezpieczone hasłem sieci Wi-Fi.

**Przede wszystkim – zachowaj zdrowy rozsądek**

Nie każde zagrożenie można przewidzieć i nie przed każdym można się obronić. Korzystając z urządzeń podłączonych do Internetu należy zawsze zachować ostrożność i postępować zgodnie ze zdrowym rozsądkiem. Gdy strona internetowa, reklama czy wiadomość e-mail wzbudzają podejrzenia, najlepiej po prostu je omijać. Stosując wszystkie wymienione wyżej zasady zmniejszymy szanse, że nasze dane, programy czy urządzenia staną się celem hakerów. Niestety nawet najuważniejsi użytkownicy mogą zostać ofiarą ataku, ale to od nas zależy jak łatwą pracę będą mieli cyberprzestępcy.

O firmie GoRepair

GoRepair to pogwarancyjny serwis naprawiający smartfony, tablety i laptopy najpopularniejszych marek. Wygodne narzędzie dostępne na stronie internetowej, umożliwia łatwe i szybkie zgłoszenie usterki oraz wybór terminu, w którym kurier odbierze urządzenie od klienta. Dla większości napraw dostępna jest natychmiastowa wycena kosztów. Typowe uszkodzenia są naprawiane od ręki, a w bardziej skomplikowanych przypadkach czas naprawy jest ustalany indywidualnie. Gwarancja udzielana na usługi wykonane przez GoRepair to 12 miesięcy.

Więcej informacji: [www.gorepair.pl](http://www.gorepair.pl)

Kontakt dla mediów

Agencja WĘC Public Relations

Tomasz Węc /PR Director
E-Mail: tomasz@wec24.pl
Telefon: 667 954 282

Łukasz Warchoł / Senior PR Executive
E-Mail: lwarchol@wec24.pl
Telefon: 535 954 212