Urodzeni w dobie Internetu lepiej radzą sobie z jego zagrożeniami

Kategoria: Styl życia
Opublikowano: środa, 27, październik 2021 13:54
Joanna Gryboś-Chechelska

Tylko niewiele ponad ¼ osób po 65 roku życia wiedziałaby, jak poradzić sobie z atakiem hakerów. Na e-zagrożenia znacznie lepiej przygotowani są ludzie młodzi. Blisko połowa z nich deklaruje, że wiedziałaby, co zrobić w przypadku ataku cyberprzestępców. Obie grupy za największe zagrożenie w sieci uznają działania oszustów wyłudzających dane poprzez fałszywe e-maile i SMS-y. Dalej są wycieki danych i ataki hakerów, których bardziej obawiają się jednak starsi. Tak wynika z badania serwisu ChronPESEL.pl i Krajowego Rejestru Długów.

29 października 1969 r. to data, którą przyjęto jako dzień narodzin Internetu. Dziś dostęp do sieci bardzo ułatwia życie. Pozwala na załatwienie spraw bankowych lub zrobienie zakupów, zapewnia dostęp do informacji i umożliwia kontakt z najbliższymi. A to zaledwie ułamek jego możliwości. Niestety, obok udogodnień, czekają tam na nas również zagrożenia. Eksperci sprawdzili, jak radzą sobie z nimi dwa pokolenia: ludzie, na oczach których rozwijał się Internet oraz ci, którzy nie znają innego świata.

Najpoważniejsze zagrożenia w sieci to obecnie phishing, ataki hakerów oraz wycieki danych osobowych. W przeprowadzonym przez serwis badaniu, zarówno najmłodsi respondenci (18-24 lata), jak i ci starsi od Internetu (65-74 lata), za największe niebezpieczeństwo uznali kradzież danych w wyniku wyłudzenia poprzez fałszywe e-maile i SMS-y. Przy czym za główne zagrożenie uważa ją aż 48 proc. najmłodszych osób i 45 proc. najstarszych.

Nieco inaczej wygląda już jednak sytuacja w grupie 55-64 lata. Ankietowani w tym wieku za największe zagrożenie (41 proc.) dla bezpieczeństwa w sieci uznali wycieki danych. Co ciekawe, wśród najmłodszych badanych obawia się tego zaledwie niespełna 19 proc. osób. Za groźne uważają z kolei ataki hakerów. Obawia się ich co trzeci (32,5 proc.) ankietowany w wieku 18-24 lata. Wśród osób pamiętających świat bez Internetu za zagrożenie uważa to zaledwie 17 proc. (ankietowani w wieku 65-74 lata) i 19,5 proc. (55-64 lata).

Udający listonoszy i kurierów zachęcają do klikania w linki

Świadomość użytkowników Internetu dotycząca zagrożenia nie zniechęca jednak do działania cyberprzestępców, którzy stale szukają nowych sposobów na to, żeby nas oszukać. Do tej pory próbowali podszywać się m.in. pod pracowników banków, Sanepidu, Poczty Polskiej lub innych firm kurierskich.

Mechanizm zawsze jest ten sam. Wszystko zaczyna się od maila lub SMS-a z wiadomością o nowej ofercie, konieczności dokonania dopłaty do przesyłki lub możliwości zapisania się na szczepienie. Po kliknięciu w link jesteśmy proszeni o podanie danych osobowych, np. numeru PESEL lub danych do logowania w banku. Udostępnienie tych informacji może się wiązać z poważnymi konsekwencjami w postaci utraty pieniędzy z konta lub koniecznością spłaty zaciągniętych na nasze nazwisko zobowiązań. Uważać musimy także na dołączone do podejrzanych e-maili załączniki.

– *Pobranie takiego pliku często inicjuje na naszym urządzeniu instalację złośliwego oprogramowania, za pomocą którego przestępcy zyskują dostęp do naszych danych. Żeby tego uniknąć, musimy bardzo uważnie weryfikować wszystkie przychodzące wiadomości, nawet jeśli na pierwszy rzut oka wyglądają one wiarygodnie. Wystarczy, że adres mailowy lub adres strony www będzie się różnił jedną literką, a swoje dane nieświadomie przekażemy cyberprzestępcom. W razie wątpliwości najlepiej samemu skontaktować się z firmą, dzwoniąc na przykład na oficjalną infolinię. Warto również zadbać o aktualne wersje systemu i programów antywirusowych na urządzeniach, z których korzystamy* – ostrzega Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl.

Jak wynika z przeprowadzonego badania w takiej sytuacji lepiej poradziliby sobie najmłodsi użytkownicy sieci. Blisko połowa z nich (47,5 proc.) deklaruje bowiem, że wie, co należy zrobić w przypadku ataku hakerów na ich komputer, tablet lub telefon. Rówieśnicy Internetu nie są tego już tacy pewni. 40,5 proc. z nich twierdzi, że umiałaby sobie z tym poradzić. Zdecydowanie najgorzej przygotowani do tego są z kolei ludzie, którzy pamiętają czasy bez Internetu. Tylko niespełna 28 proc. ankietowanych w wieku powyżej 65 r.ż. wiedziałaby, co zrobić w przypadku ataku hakerów.

Starsze pokolenie zapisuje hasła w notesie

Ważną zasadą bezpieczeństwa w sieci jest umiejętne zarządzanie hasłami do logowania. W tym aspekcie dużo większą roztropnością wykazują się osoby, które pamiętają świat bez Internetu. Ponad 60 proc. ankietowanych po 65 r.ż. i 56 proc. badanych w wieku 55-64 lata deklaruje bowiem, że nie używa tego samego hasła w kilku serwisach. W przypadku najmłodszych ten odsetek wynosi zaledwie niespełna 40 proc. Co więcej, połowa tej grupy respondentów otwarcie przyznaje się do tego, że ustawiła sobie to samo hasło w kilku różnych miejscach.

Pewność siebie młodych może wynikać z tego, że z reguły ustawiają trudniejsze do złamania hasła niż starsze pokolenie. Ponad ¾ z nich deklaruje bowiem, że korzysta z silnych haseł. Tak samo może powiedzieć zaledwie 57 proc. ankietowanych w wieku powyżej 65 r.ż. i niespełna 2/3 badanych w grupie 55-64 lata.

– *Nawet skomplikowane hasło nie zagwarantuje nam bezpieczeństwa, jeśli będziemy go używać w kilku serwisach. Wystarczy bowiem, że dojdzie do wycieku danych z jednego z nich, żeby cyberprzestępcy zdobyli klucz do naszych pieniędzy. Z drugiej strony korzystamy dziś z bardzo wielu serwisów i nie jesteśmy w stanie wymyślić i pamiętać tak dużej liczby haseł. Rozwiązaniem jest używanie jednego z szyfrowanych programów do ich przechowywania. Paradoksalnie jedną z najbezpieczniejszych metod może okazać się również zapisywanie haseł w zwykłym notesie. Oczywiście pod warunkiem, że trzymamy go domu* – tłumaczy Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl.

Z tego sposobu korzysta 40 proc. najmłodszych respondentów. Dodatkowo 30 proc. z nich zapisuje hasła w telefonie, a co piąty w komputerze. Mniej zaufania do nowoczesnych narzędzi mają najstarsi ankietowani. Około 70 proc. z nich trzyma dane do logowania w notesie i to jedyna metoda, której ufają.

Źródło: IP