Miasto. Tygodnik Koszaliński
29.07.22 nr: 30 str. 6 nakład: 10000 egz.

Sposób na hakera

Internet może nieść ze sobą tyle samo przyjemności, co zagrożeń. A musimy być na nie dobrze przygotowani, bo coraz więcej spraw załatwiamy w sieci, co oznacza, że nie tylko nasze dane osobowe są na wyciągnięcie ręki. Może oberwać także nasz sprzęt – komputer, laptop, tablet czy smartfon, i pliki, które na nich przechowujemy. Co nam obecnie zagraża? Jakie błędy popełniamy, a przede wszystkim – jak się bronić?

Alicja Tułnowska

Niestety, nikt nie może czuć się w sieci w 100 procentach bezpieczny, co potwierdza dr Krzysztof Kaczmarek z Wydziału Humanistycznego Politechniki Koszalińskiej, specjalista w temacie cyberbezpieczeństwa. Dodaje jednak, że można zwiększyć poczucie własnego bezpieczeństwa, stosując m.in. odpowiednie oprogramowanie i zachowując zdrowy rozsądek.

Obecnie tych zagrożeń jest zdecydowanie więcej niż kiedyś, na co wpływ ma też po części to, że o wiele więcej spraw załatwiamy zdalnie. Co więcej, jak twierdzi dr Kaczmarek, podatność na ataki internetowe jest bardziej związana z kwestią świadomości zagrożeń niż z wiekiem. – Często jest tak, że osoby starsze mówią, że ich syn czy córka są dobrzy w internecie, bo siedzą w nim godzinami i „wszystko" potrafią zrobić, ale to „wszystko" ogranicza się do wrzucania jakichś informacji na mediach społecznościowych – zdjęć, filmów itd.

Inaczej należy spojrzeć na problem zagrożeń u dzieci. – Możemy poczytać sobie w podręcznikach do psychologii, że myślenie abstrakcyjne o możliwych skutkach własnych postępowań pojawia się dopiero z wiekiem. Dziecko jest podatne bardzo na zagrożenia, dlatego że nie zdaje sobie sprawy z tych zagrożeń – wyjaśnia ekspert. – Czasem powinno się z takimi dziećmi porozmawiać, ale nie powinni tego robić rodzice, tylko osoby nieco starsze np. o pięć lat, które już czują jakąś odpowiedzialność.

Narzędzia destrukcji

To w dużej mierze od nas zależy, czy wygramy z licznymi zagrożeniami, czy staniemy się ofiarą. Z czym walczymy? To m.in. wirusy, robaki czy trojany. Co mogą zrobić? M.in. wyświetlają reklamy czy strony, których nie chcemy, spowalniają nasze urządzenia, mogą niszczyć pliki czy wysyłać SPAM z poczty. Niektóre potrzebują do działania podłączenia do internetu, inne atakują nasz sprzęt przez zainfekowane programy. Mamy jeszcze takie zagrożenie jak np. spyware, które szpiegując, ma za zadanie wykraść nasze dane – nie tylko te do bankowości, ale też hasła do różnych kont, historię. Adware natomiast atakuje nas przez reklamy, które mogą pojawić się w nadmiernej liczbie, co znacznie utrudnia korzystanie z urządzenia. Obecnie nie tylko haker osobiście czyha w sieci, by nieco utrudnić nam życie i zabawić się naszym kosztem lub się na nas wzbogacić. Teraz mamy do czynienia także z botami, czyli programami, które przejmują ich działania. Żeby to jednak zadziałało, popełnić błąd. Jak ich uniknąć?

Ochrona

Specjalista podkreśla, że najważniejszą ochroną przed zagrożeniami w sieci jest dobry antywirus. Przestrzega jednak przed poleganiem na darmowych wersjach – jak czyni wielu użytkowników. Warto wybrać jedną z dogodnych dla nas opcji oferowanych przez dobre antywirusy, które ochronią nas nie tylko przed wirusami, ale również pozostałymi zagrożeniami (mogą też monitorować darknet – nazywany ciemną stroną internetu, gdzie dochodzi do wielu nielegalnych działań z zachowaniem anonimowości). Jeśli mamy wątpliwości, nie jesteśmy pewni, jakiego rodzaju ochrony potrzebujemy, to zawsze warto poradzić się eksperta np. w sklepie czy w serwisie komputerowym albo znajomego informatyka.

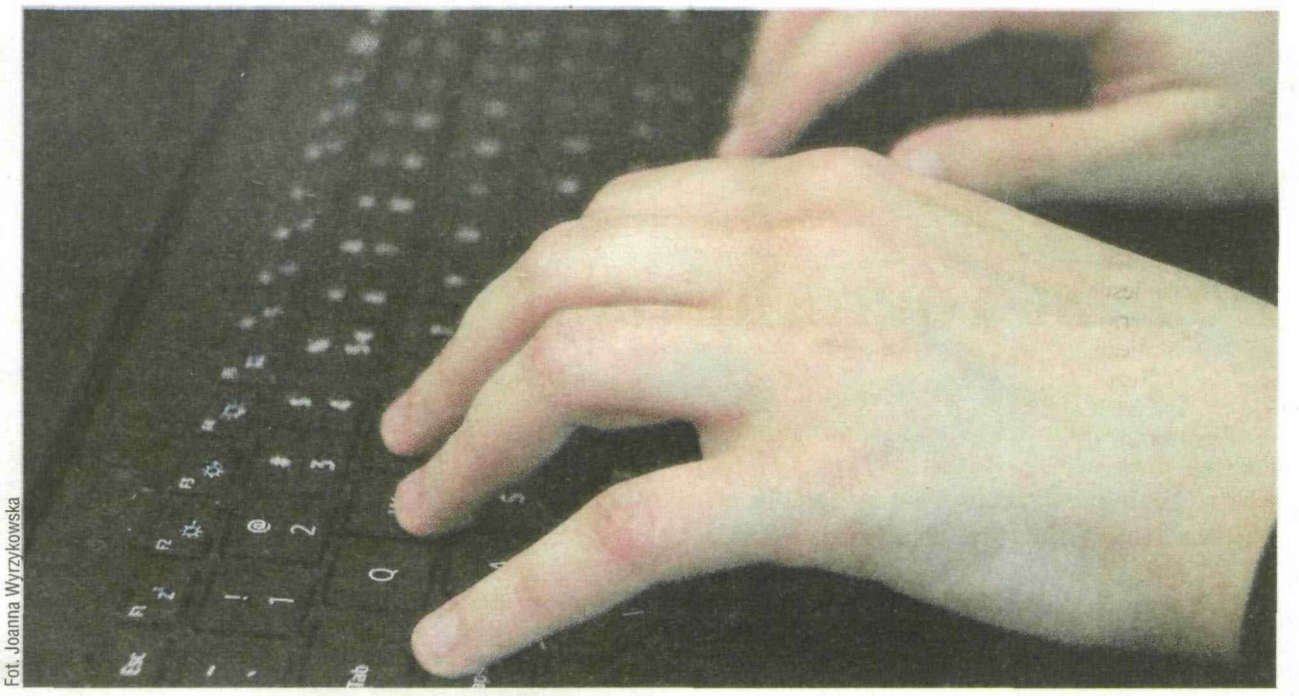
Mówiąc o oprogramowaniu antywirusowym, zwykle myślimy o komputerach stacjonarnych czy laptopach, jednak należy mieć również na uwadze, że tak samo silnej ochrony potrzebują również inne urządzenia podłączane do sieci, jak tablety czy smartfony. Oprócz antywirusa można też skorzystać z VPN, czyli z wirtualnej sieci prywatnej, która pozwala m.in. na ukrycie adresu IP i chroni naszą tożsamość online, szyfrując nasze połączenie. Mamy taką opcję nawet w systemie Windows.

Choć odpowiednie programy zabezpieczające w dużym stopniu przejmują ochronę naszych urządzeń i danych, to nie zwalnia nas to jednak z obowiązku bycia ostrożnym. Warto zwracać uwagę na pewne niepokojące nas, nawet te najsubtelniejsze, sygnały. To nie tylko adres strony internetowej (w bankowości zwracajmy też uwagę na to, aby widoczna była kłódka w wyszukiwarce), ale też inna szata graficzna. Jak zaznacza dr Kaczmarek, powinniśmy zachować ostrożność, jeśli zauważymy nawet niewielką zmianę odcienia strony internetowej (np. jaśniejszy kolor). O potencjalnym niebezpieczeństwie mogą również świadczyć nieprawidłowości językowe na znanych nam stronach (brak polskich znaków, złe tłumaczenia czy niepoprawny szyk zdania). Nie klikajmy w podejrzane linki, a przy odbieraniu poczty zwracajmy szczególną uwagę nie tylko na temat, ale również na adres nadawcy. Co więcej, bez odpowiedniej ochrony możemy zostać przekierowani na stronę oszustów podczas logowania np. do bankowości, a wtedy nietrudno o utratę oszczędności.

Niestety, jak twierdzi ekspert, nawet specjaliści z branży mają problem, by wychwycić wszystkie możliwe zagrożenia, ale uspokaja, że nie powinniśmy wpadać w paranoję w kwestii grożących nam niebezpieczeństw i ochrony. – Najłatwiej zabezpieczyć się przed hakerami po prostu zachowując zdrowy rozsądek, nie wpadając w panikę. Nie to, że odcinamy się od razu od sieci, bo nie możemy – dodaje.

Zakryte kamerki

Kilkanaście lat temu pojawiły się słynne plastry na kamerkach np. laptopów w lęku przed kompromitującym nagraniem. Wiele osób doskonale to pamięta i być może do dzisiaj zastanawia się, czy rzeczywiście miało to sens. Nawet nasz ekspert uważał wtedy takie zachowanie za paranoiczne. Zagrożenie to było prawdziwe i także dzisiaj jest realne, zwłaszcza w warunkach wojennych. – Większość portali rosyjskich jest wyłączonych na terenie Europy, więc żeby to ominąć, są różne portale randkowe czy inne dla dorosłych, gdzie ludzie nawiązują kontakt i nawet klikając w link, żeby połączyć się przez kamerę i z kimś poczatować, infekują swój sprzęt – wyjaśnia dr Kaczmarek. – Kamery można włączyć.



Fot. Joanna Wyrzykowska

Nie potrzeba tutaj wyrafinowanego oprogramowania. Jeżeli ktoś nie ma profesjonalnego programu antywirusowego, a ma darmowy – to tak, jakby go nie było. Kamera czy mikrofon mogą zostać włączone nawet bez naszej świadomości.

Specjalista zwraca również uwagę, że w przypadku nagrania może pojawić się ryzyko szantażu. – Jedyne, co ja mogę poradzić, jeżeli ktoś się odzywa i próbuje szantażować, to zgłosić to na policję i się tym nie przejmować – no, trudno. Można stracić kontrolę nad własnym życiem – wyjaśnia. – Takie rzeczy się działy, że ktoś w darknecie kupił narkotyki w promocyjnej cenie i teraz spędza kilka lat w południowoamerykańskim więzieniu, bo ktoś nagrał, jak on to kupował. I poszło dalej. A mógł po prostu zgłosić się na policję.

Wi-Fi

Chętnie logujemy się do darmowego internetu w najróżniejszych miejscach przez Wi-Fi. I nie jest to nic nadzwyczajnego. To wręcz wymóg – wszędzie oczekujemy tego połączenia – w wynajętym apartamencie na wczasach, w kawiarniach, na dworcach, na uczelni czy w centrum handlowym. Szukamy darmowego internetu, gdzie się tylko da. Niestety, za to przyzwyczajenie możemy słono zapłacić, ponieważ sieć Wi-Fi to idealne środowisko np. dla hakerów, a ci czyhają m.in. właśnie na nasze hasła. W dodatku nie możemy czuć się całkowicie bezpieczni także w sieci domowej. Tu za nietypowy przykład ekspert podaje osoby pracujące w zawodach mających dostęp do danych wrażliwych (m.in. dane studentów, dane ewidencyjne kierowców, numery PESEL). Muszą oni liczyć się z możliwością odpowiedzialności karnej w przypadku przechwycenia hasła.

Dr Kaczmarek radzi, by zachować szczególną ostrożność podczas logowania się do sieci Wi-Fi poza domem i nie łączyć się z sieciami nieznanymi. Poleca za to użycie danych komórkowych na smartfonie. – Jeśli nasze urządzenie jest ustawione, że loguje się do sieci Wi-Fi, która jest automatycznie otwarta, to tak naprawdę udostępniamy wtedy całą zawartość do urządzenia, łącznie z możliwością odczytania treści, które dawno wykasowaliśmy – zwłaszcza chodzi o treści multimedialne – zdjęcia, filmy, nagrania głosowe.

Dodatkowo, specjalista przestrzega też, by zwracać uwagę na treści pozostawiane przez nas w internecie – zdjęcia, a nawet komentarze. Przypomina, że nawet jeśli je usuniemy, to i tak ktoś może znaleźć do nich dostęp, bo w internecie nic nie ginie.

Hasła i logowanie

Obecnie dobrym rozwiązaniem jest nie tylko ustawienie hasła, ale utworzenie weryfikacji kilkustopniowej, gdzie przy okazji logowania (np. na nieznanym urządzeniu) zostajemy poproszeni o wpisanie dodatkowego kodu, który przychodzi do nas np. w SMS-ie, w e-mailu czy przez aplikację autoryzacyjną zmieniającą co kilka sekund kod dostępu. Dodatkowo, jeśli korzystamy z nieznanego nam urządzenia, warto użyć dostępnego w przeglądarce internetowej trybu anonimowego, incognito czy prywatnego (in private). – Wtedy po zamknięciu przeglądarki żadne hasła nie są zapisywane, ciasteczka też – dodaje ekspert.

Jak to jest jednak z tymi hasłami? Tu dr Kaczmarek radzi, by zmieniać je regularnie. Jak często? Specjalista zauważa, że m.in. niektóre banki radzą robić to co tydzień, a niektórzy co miesiąc. Ponadto, jeśli zalogowaliśmy się w miejscu niezaufanym, także warto rozważyć zmianę haseł. Tu przede wszystkim należy wziąć pod uwagę takie trudne do odgadnięcia – nawet wiele aplikacji, usług ma wymóg, by hasło było długie, zawierało cyfry, litery małe i duże, a także znaki specjalne. Nie powinny ono nawiązywać np. do daty urodzenia czy imienia bliskiej nam osoby, pupila.

A co jeśli ktoś przejmie nasz klucz do sieci domowej? – To ma możliwość, żeby poszperać po naszych urządzeniach – mówi dr Kaczmarek. – Nie sądzę, by przeciętny użytkownik internetu był obiektem zainteresowania specjalistów z dziedziny hakerstwa. Przyczyną tutaj może być zwykła złośliwość. To może być uczeń siódmej, ósmej klasy, który postanowił się w hakerstwo pobawić.

Ekspert odradza, by używać wszędzie takiego samego hasła, ale przyznaje, że niełatwo jest poradzić sobie z zapamiętaniem ciągle zmienianych haseł. Uważa to za niemożliwe i opowiada, że jemu też zdarzyło się pomylić hasła (PIN do karty z kodem do domofonu), a w rezultacie musiał wymienić kartę bankomatową na nową...

Jest jeszcze jedna kwestia, przed którą przestrzega specjalista. – Jak wpisujemy hasło, to nie mówić go głośno. Spotkałem się z tym na zajęciach. Nie róbmy tego... – apeluje.

Co, gdy ktoś jednak przejmie nasze hasło, a przez to postanowi z skorzystać z naszych danych? – Niestety, w naszym systemie prawnym jest tak, że jeżeli staniemy się ofiarą przestępstwa, np. udowodnimy, że ktoś się logował z południa Polski, a my jesteśmy nad morzem i ten ktoś na nasze dane wziął kredyt, to możemy to zgłosić i tę osobę ścigać, a komornik i tak z nas ściąga. Po prostu każda instytucja finansowa dba przede wszystkim o swój interes... – przestrzega dr Kaczmarek. ■