IM WIĘCEJ INTERNETU, TYM BARDZIEJ WARTO ZADBAĆ O PRYWATNOŚĆ

O wpływie Internetu i nowych technologii na kształtowanie bezpiecznych zachowań w sieci z dr. Sylwestrem Bębasem rozmawia Ewelina Janczylik-Foryś

Sylwester Bębas - doktor nauk społecznych, nauczyciel akademicki, psychoterapeuta, pedagog, profilaktyk specjalizujący się w uzależnieniach od świata wirtualnego i bezpiecznych zachowaniach w sieci, trener kompetencji medialnych, wychowawczych i interpersonalnych

Nowoczesne technologie informacyjne, których symbolem stał się komputer i Internet, budzące zainteresowanie wszystkich grup wiekowych. Z przeprowadzonego badania „Ochrona danych osobowych w 2022 r". wynika, iż młodzi ludzie uważają, że wszystko wiedzą o nowych technologiach, a osoby nieco starsze już niekoniecznie. Czy Pana zdaniem raport prawidłowo ocenia zachowania i świadomość grup wiekowych?

– Żyjemy w świecie, w którym ludzie powszechnie korzystają z Internetu. I nic w tym dziwnego, bowiem Internet służy do różnych celów do pracy, nauki, rozrywki, komunikacji itp. Używany jest przez osoby w różnym wieku, z różnym wykształceniem. Oprócz zalet niesie ze sobą wiele zagrożeń. Codziennie wykradanych jest wiele milionów rekordów, pojawia się też wiem prób instalowania złośliwe oprogramowania. Dane użytkowników sieci stały się cennym towarem na rynku cyberprzestępczym. Zakupem takich informacji zainteresowani są także tzw. brokerzy danych. Skupują oni informacje o ludziach, aby później sprzedać je zainteresowanym firmom. Raport jest spójnym wartościowym dokumentem podnoszącym świadomość na temat bezpieczeństwa danych osobowych w Polsce przeprowadzonym na reprezentatywnej grupie badanych. Raport ukazuje najważniejsze zagrożenia, niebezpieczne zachowania, konsekwencje utraty danych osobowych, działania profilaktyczne, zachowania Polaków w tym zakresie, ma wartość diagnostyczną, edukacyjna i profilaktyczną. Przekonanie młodych ludzi o tym, że wszystko wiedzą o nowych technologiach jest złudne, dlatego potrzebna jest edukacja medialna wszystkich grup wiekowych.

Bardzo ważną rolę w zapewnieniu bezpieczeństwa swoim dzieciom odgrywają rodzice, którzy powinni mieć świadomość zagrożeń, z którymi może spotkać się dziecko w sieci, oraz dysponować wystarczającą wiedzą i umiejętnościami, aby zadbać o to bezpieczeństwo. Rodzice powinni: ograniczać czas spędzany przez dzieci w sieci, rozmawiać z dzieckiem na temat bezpiecznego korzystania z Internetu, kontrolować i nadzorować aktywność dziecka w sieci, sprawdzać strony, na które zagląda dziecko, ustalić reguły, zasady i ograniczenia związane z dostępem do Internetu. Podniesienie poziomu bezpieczeństwa dzieci on-line zależy również od dostawców usług internetowych i producentów sprzętu elektronicznego oraz oprogramowania. Rozwiązania technologiczne w dużym stopniu mogą wpływać na poziom bezpieczeństwa dzieci on-line i mogą stanowić dla opiekunów młodych internautów pomoc w czuwaniu nad ich bezpieczeństwem.

90 procent Polaków deklaruje, że wie, jak zadbać o bezpieczeństwo swoich danych osobowych. Najpewniej czują się ludzie młodzi. Pomimo przekonania o swojej wiedzy, to oni są jednak grupą, która najczęściej popełnia błędy w postaci publikacji zdjęć swoich dokumentów w sieci lub udostępnia osobom trzecim loginy i hasła. Jednak młodzi ludzie nie są tacy uświadomieni jak im się wydaje…

– Dlatego potrzebna jest stała edukacja zwłaszcza na temat podstawowych zasad bezpieczeństwa. Po pierwsze, nie powinno używać się tego samego loginu i hasła do wielu usług i serwisów. Po drugie, myśleć o tym, komu i w jakim celu udostępniamy nasze dane. Nie każdy serwis musi wiedzieć o nas wszystko. Już w momencie podawania rozmaitych danych podczas rejestracji niekiedy powinno zapalić się nam w głowie czerwone światło ostrzegawcze. Po trzecie, jeżeli mamy taką możliwość, zawsze powinniśmy korzystać z uwierzytelniania dwuetapowego (np. potwierdzenie logowania kodem SMS, odciskiem palca czy korzystać z systemu rozpoznawania twarzy). Warto też uświadamiać jakie dane te zwykłe i te wrażliwe chronić. Należy zwrócić uwagę na: imię i nazwisko, numer identyfikacyjny (np. PESEL, NIP, numer dowodu osobistego), adres zamieszkania, adres mailowy, datę urodzin, płeć, kolor oczu, waga, wzrost, dane ujawniające pochodzenie rasowe
lub etniczne, dane ujawniające poglądy polityczne, dane ujawniające przekonania religijne lub światopoglądowe, dane ujawniające przynależność do związków zawodowych, dane genetyczne, dane biometryczne (wykorzystywane w celu jednoznacznego zidentyfikowania osoby fizycznej), dane dotyczące zdrowia itp.

Czy Polacy są w stanie sami zadbać o swoje dane osobowe? Zawsze utrata kontroli nas danymi osobowymi to efekt ataków socjotechnicznych. Jedyne co może różnić to sposób działania.

– Dlatego należy edukować, zachęcać do czytania regulaminów. Dość często sami wyrażamy zgodę na to, aby nasze dane, które przesyłamy w jakieś miejsce w sieci lub udostępniamy określonej aplikacji lub serwisowi internetowemu, były udostępniane lub odsprzedawane innym osobom lub firmom. Informacje

o tym znajdują się właśnie w regulaminach. Warto czytać na co zgadzamy się, akceptując zgodę na działanie ciasteczek. Są one w zasadzie niezbędne do prawidłowego funkcjonowania stron internetowych. Poprawiają nasz komfort użytkowania różnych portali i serwisów. Informują też nadawców, jakie treści cieszą się większym, a jakie mniejszym zainteresowaniem. Zresztą zazwyczaj jesteśmy o nich informowani po wejściu pod konkretny adres w sieci. Nie ma w nich nic złego. Zanim na kolejnej stronie zaakceptujecie jednym kliknięciem wszystkie zgody na działanie „ciasteczek", wczytajcie się dokładnie, czego one dotyczą. Pewnie warto poświęcić kilka sekund więcej i dostosować stosowne zgody do własnych potrzeb. Za każdym razem, gdy instalujemy nową aplikację na telefonie lub tablecie, rejestrujemy się do nowego serwisu czy usługi, należy uważnie przeczytać regulamin i zastanowić się, na co właściwie się zgadzamy.

W jaki sposób zachęcić Polaków, w tym zwłaszcza osoby starsze, których technologie cyfrowe nie są aż tak bliskie, do tego, aby jeszcze większą uwagę zwrócili na potrzebę bezpiecznego posługiwania się własnymi danymi osobowymi w codziennych sytuacjach?

– Przede wszystkim uświadamiać, że w sieci użytkownik Internetu narażony jest na różnego rodzaju oszustwa, które mają na celu np. okradzenie, oszukanie lub wykorzystanie danej osoby. Jedną z metod cyberoszustwa jest tzw. phishing – przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji np. danych logowania czy danych karty kredytowej, następuje zainfekowanie urządzenia szkodliwym oprogramowaniem i nakłonienie ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej. Jeszcze inną formą oszustwa jest spear phishing, czyli cyberpolowanie z harpunem na wybraną osobą. O ile w przypadku phishingu zarzucana najczęściej jest sieć, z nadzieją, że złapią się na nią jakieś ofiary, tak w przypadku spear phishingu cyberprzestępca poluje na jedną, konkretną ofiarę. Z kolei clone phishing jest typem phishingu, w którym prawdziwy e-mail posiadający załącznik lub link zostaje użyty przez przestępcę jako wzór przy tworzeniu wiadomości na potrzeby oszustwa. Załączniki lub linki zostają zastąpione złośliwymi wersjami, a następnie wysłane z adresu e-mail sfałszowanego tak, aby wyglądał jak ten należący do nadawcy. Whaling jest z kolei oszustwem, gdzie część ataków phishingowych zostaje skierowana w szczególności do kierownictwa wyższego szczebla lub jest ukierunkowana na pozyskanie informacji z branży biznesowej objętych tajemnicą. W przypadku ataków tego typu, sfałszowana witryna lub wiadomość jest tworzona z uwzględnieniem np. stanowiska jakie zajmują ofiary ataków w firmie. Treść e-maili często przypomina pisma pochodzące z kancelarii prawnych lub urzędów państwowych. Taka wiadomość może zawierać załącznik w postaci złośliwego oprogramowania i nakłaniać ofiarę do jego instalacji np. w celu uzyskania dostępu do ważnego dokumentu. Cyberoszuści mogą proponować także fałszywą pomoc techniczną, w której przestępca próbuje zastraszyć ofiarę i skłonić ją do zapłacenia za zbędną pomoc techniczną. Metoda ta wykorzystuje brak wiedzy informatycznej ofiary. Pharming jest bardziej niebezpieczną dla użytkownika oraz trudniejszą

do wykrycia formą phishingu. Charakterystyczne dla pharmingu jest to, że nawet po wpisaniu prawidłowego adresu strony WWW, ofiara zostanie przekierowana na fałszywą, choć mogącą wyglądać tak samo, witrynę internetową. Ma to na celu przejęcie haseł, numerów kart kredytowych i innych poufnych danych wpisywanych przez użytkownika do zaufanych witryn. Z pharmingiem związany jest drive-by pharming, który jest formą zagrożenia internetowego, będącą połączeniem ataku typu pharming, jak i socjotechniki. Celem agresora jest skłonienie ofiary do odwiedzenia przygotowanej wcześniej strony internetowej, zawierającej szkodliwy kod, który ma za zadanie zmianę ustawień na routerze osoby odwiedzającej w taki sposób, że adresy wpisywane przez użytkownika, będą przekierowywane na strony spreparowane przez atakującego. Jeszcze inne oszustwo typu scam polega na wzbudzeniu u kogoś zaufania, a następnie wykorzystanie tego zaufania
do wyłudzenia pieniędzy lub innych składników majątku. Osoba wzbudzająca fałszywe zaufanie zwykle działa na jedną z ludzkich cech charakteru, zarówno negatywnych, jak i pozytywnych, takich jak: pycha i chciwość, ale też empatia i altruizm. Jest jeszcze SMS phishing, czyli atak socjotechniczny podobny do phishingu, polegający na rozsyłaniu SMS-ów, które mają skłonić ofiarę do podjęcia określonego działania.

Bardzo często podkreślamy, jak ważna jest edukacja i budowanie odpowiednich postaw wśród użytkowników nowych technologii. Często jednak korzystając z nowoczesnych rozwiązań, nie wiemy jak one działają. Co prawda, co jakiś czas aktualizujemy oprogramowanie w telefonie, ale nie wiemy dlaczego – pewnie dla poprawy funkcjonowania.

– Niestety często nie wiemy, jak działają nowe technologie, dlatego zasady bezpieczeństwa są tu kluczowe. Bardzo ważne jest, aby stosować zasady bezpieczeństwa podczas komunikowania się przez Internet. Nie powinno się rozmawiać z nieznajomymi, poza przypadkami uzasadnionymi np. sprzedawcą w sklepie internetowym, lekarzem itd. Wszystkie osoby, z którymi nawiązywany jest kontakt w sieci nie powinny być anonimowe, tzn. nieznane z imienia i nazwiska. W żadnym wypadku nie powinno się wysyłać nieznajomym plików, w tym zdjęć i filmów, przesyłać spamu, w tym tzw. łańcuszków szczęścia czy otwierać wiadomości z podejrzanymi linkami, które mogą zawierać wirusy i posłużyć do okradzenia danej osoby. Bardzo ważne jest, aby korzystając z Internetu stosować zasady netykiety, która jest rodzajem niepisanych, ale przyjętych i przestrzeganych przez internautów zasad korzystania z sieci m.in. zasad komunikowania się w sieci, jest to rodzaj internetowego savoir-vivre'u. W sieci, tak jak w każdej społeczności, istnieją reguły zachowania się, których należy przestrzegać. Nieprzestrzeganie ich może skutkować uwagami ze strony administratora i innych użytkowników, wykluczeniem z grupy, a nawet całkowitym zablokowaniem dostępu do usług. Bardzo ważne jest korzystanie z Internetu stosować szyfrowanie, które służy do zachowania poufności danych. Plik lub przesyłane dane są zniekształcane tak, że tylko właściwe osoby posiadające tajny „klucz" mogą odtworzyć oryginalny tekst. Gdy ktoś korzysta z urządzeń cyfrowych, cały czas używa systemów opartych

na szyfrowaniu: kiedy korzysta z bankowości internetowej, łączy się z siecią Wi-Fi, płaci kartą płatniczą. Wokół prawie każdej czynności w sieci pojawia się szyfrowanie. Dlatego korzystając z poczty, banku lub sklepu internetowego oraz wszystkich stron, na których podaje się swoje dane (login i hasło), należy sprawdzać, czy połączenie jest szyfrowane. Połączenie szyfrowane jest wtedy gdy, w pasku adresu znajduje się kłódka i napis: „https", gdzie „S" oznacza secure, czyli bezpieczny. Ważne jest, aby urządzenia elektroniczne, z których korzystamy chronić odpowiednim oprogramowaniem, które ułatwia identyfikację zagrożenia wirusowego i pozwala te wirusy skutecznie zwalczać. Wirusy infekują urządzenie gdy ktoś otwiera pocztę od nieznajomych. Najczęściej są to załączniki, które wcale mogą nie wyglądać groźnie. Cyberprzestępcy podszywają się także pod różne instytucje i organizacje. Niebezpieczne jest pobieranie plików z nielegalnie rozpowszechnionymi filmami, grami, programami, aplikacjami, książkami, a niekiedy także z muzyką. Instalując oprogramowanie nie należy klikać w link w wyskakującym okienku z informacją, aby pilnie coś zainstalować. Takie wyskakujące okienka często są pułapką. Linki, które są w nich zawarte, uaktywniają na urządzenie pliku ze złośliwym oprogramowaniem.

Czy powinniśmy się z tym pogodzić, że nie jesteśmy w stanie nadążyć za nowymi rozwiązaniami i po prostu polegać na ogólnych rekomendacjach?

– Internet doprowadził nie tylko do implozji przestrzeni i czasu, ale także znaczeń. Praktycznie wszystko w nim jest akceptowalne i prawie nic nie jest trwałe. Sprzyja to relatywistycznemu sposobowi myślenia. Wzmacnia to niewątpliwie coraz powszechniejszą tendencję do unikania odpowiedzialności osobistej i zaangażowania. Wzrastająca liczba użytkowników Internetu oraz rozwój on-line różnych aspektów ludzkiej działalności dotyczącej wszystkich niemalże sfer życia ludzkiego powoduje, że coraz trudniej wyznaczyć linię demarkacyjną, dzielącą życie wirtualne od życia realnego. Jesteśmy świadkami niebywałego rozwoju technik i technologii teleinformatycznych. Patologie w cyberświecie to nie tylko wyłącznie uzależnienia, ale także inne niebezpieczeństwa i zagrożenia w tym cyberoszustwa i manipulacje. Wraz z rozwojem informatyzacji pojawiły się nowe problemy związane z niewłaściwym zastosowaniem osiągnięć elektronicznego przetwarzania danych. Od pewnego czasu rejestruje się olbrzymie zainteresowanie grup przestępczych wykorzystywaniem infrastruktury sieciowej, jako nowego instrumentu nielegalnej działalności. Obecnie do podstawowych obszarów obejmujących nadużycia w Internecie należą przede wszystkim: ukrywanie tożsamości, nawiązywanie nielegalnych konwersacji/komunikacji, dystrybuowanie nielegalnych materiałów, gry hazardowe, pranie (brudnych) pieniędzy oraz wszelkie działania mające na celu przyniesienie korzyści. Rozszerza się zjawisko kradzieży i wyłudzania danych, a także cyberoszustw i manipulacji. Dlatego powinniśmy systematycznie podnosić nasze kompetencje medialne, być świadomymi i odpowiedzialnymi użytkownikami nowych technologii.

Język wypowiedzi, w jakim są kierowane do użytkowników komunikaty, jest dość trudny. Czy ludzie w ogóle rozumieją język nie tylko RODO, ale wszystkich wiadomości, jakie kierują do na nich administratorzy, deweloperzy aplikacji mobilnych? Jak informować użytkowników o przysługujących im prawach czy o możliwych zagrożeniach?

– Przede wszystkim edukować, uczyć o tych prawach i o możliwych zagrożeniach. Tego, że korzystając z Internetu nie powinno się używać się tego samego loginu i hasła do wielu usług i serwisów. Należy myśleć o tym, komu i w jakim celu udostępnia się dane. Nie każdy serwis musi wiedzieć wszystko o jego użytkowniku. Jeżeli jest taka możliwość, zawsze powinno się korzystać z uwierzytelniania dwuetapowego np. potwierdzenia logowania kodem SMS, odciskiem palca czy korzystać z systemu rozpoznawania twarzy. Należy być ostrożnym z publikowaniem zdjęć. Nie powinno się publikować w sieci zdjęć, na których ktoś jest niekompletnie ubrany, zdjęć wnętrz mieszkań, zdjęć drogich przedmiotów, zdjęć z wakacji czy zdjęć z prywatnych spotkań. Korzystając z sieci, należy czytać regulaminy. Dość często ludzie sami wyrażają zgodę na to, aby ich dane, które przesyłają w jakieś miejsce w sieci lub udostępniają określonej aplikacji lub serwisowi internetowemu, były udostępniane lub odsprzedawane innym osobom lub firmom. Informacje o tym znajdują się właśnie w regulaminach. Za każdym razem, gdy ktoś instaluje nową aplikację na telefonie lub tablecie, rejestruje się do nowego serwisu czy usługi, powinien uważnie przeczytać regulamin i zastanowić się, na co właściwie się zgadza. Korzystając z sieci należy tworzyć bezpieczne hasła. W dzisiejszym świecie Internetu haseł używamy w zasadzie bez przerwy, przy logowaniu do poczty elektronicznej, bankowości online, dokonując zakupów lub uzyskując dostęp do rozmaitych urządzeń itp. Użytkownicy Internetu, aby łatwiej zapamiętać hasła, używają haseł krótkich, łatwo kojarzących się np. z imieniem swoich zwierząt, bohaterów z filmów, z datą swoich urodzin itp. Takie hasło niestety możne być złamane w kilka sekund. Tymczasem silne hasło nie powinno być słownikowym wyrazem, ale powinno zawierać długi ciąg dużych i małych liter, cyfr i znaków specjalnych. Bardzo dobrym rozwiązaniem podczas korzystania z Internetu jest tzw. uwierzytelnianie wielopoziomowe czyli sposób zabezpieczenia oraz autoryzacji podczas logowania przed skorzystaniem z konta użytkownika przez niepowołane osoby poprzez zdobycie przez nią identyfikatora użytkownika i hasła uwierzytelniającego. Oprócz podania tych danych logowania, użytkownik musi: podać uzyskany kod lub frazę np. ze swojego przenośnego urządzenia internetowego, poprzez przepisanie go z e-maila wysłanego przez serwis, na którym użytkownik próbuje się zalogować, czy też za pomocą specjalnej karty, linii papilarnych palca itp.

Pandemia COVID-19 narzuciła nam konieczność zastosowania e-rozwiązań. Czego się nauczyliśmy przy korzystaniu z e-usług?

– Internet w pandemii okazał się ogromnym dobrodziejstwem dla ludzi, a także dla firm działających on-line. Pierwszą zmianą jest wzrost w obszarze komunikacji – wirtualne kontakty – wideokonferencje, media społecznościowe - niemal zastąpiły komunikację bezpośrednią. Problem mają jednak osoby, które

są cyfrowo wykluczone, a jest ich w Polsce około kilkanaście procent.
Internet wpłynął znacząco na edukację – np. wprowadzono platformy edukacyjne dzięki, którym możliwe było nauczanie na odległość. W czasach pandemii coraz większą rolę zaczęły odgrywać zakupy on-line, nawet w takich branżach jak spożywcza, do tej pory zarezerwowana do zakupów stacjonarnych.
Wzrosty notowały także branże związane ze zdrowiem i urodą, książkami i multimediami, ubraniami, zabawkami. Warto zwrócić uwagę na rozwój bankowości elektronicznej: osoby starsze uczyły się dokonywania płatności, robienia przelewów czy korzystania z aplikacji mobilnych. Sprawy urzędowe – coraz więcej osób korzysta
z platformy e-Polak potrafi!, by załatwić różne sprawy urzędowe, np. złożyć wniosek o dowód. Rozwiązanie takie jak e-PIT dale nam z kolei możliwość rozliczenia się z fiskusem przez Internet. Aplikacje mObywatel, Profil Zaufany czy Internetowe Konto Pacjenta to internetowe aplikacje, dzięki którym w łatwy, szybki i bezpieczny sposób odnajdziesz informacje o swoich danych medycznych, e-skierowania, e-recepty. System eWUŚ - umożliwia łatwe potwierdzenie prawa do leczenia w ramach ubezpieczenia w NFZ. Serwis Zintegrowany Informator Pacjenta – udostępnia zarejestrowanym użytkownikom historyczne dane o ich leczeniu i finansowaniu leczenia, gromadzone od 2008 roku przez NFZ. Portal kolejkowy – umożliwia sprawdzenie najszybszego wolnego terminu wizyty u lekarza lub w szpitalu. Mamy do czynienia z przyspieszeniem transformacji cyfrowej. Szacuje się, że proces, który trwałby kilka lat, dzięki pandemii dokonał się w ciągu kilku miesięcy.

Jakie Pana zdaniem są trendy na najbliższe lata? Czy społeczeństwo będzie dążyło do ochrony prywatności, do stosowania odpowiednich zabezpieczeń, aby chronić informacje o sobie? Czy może wręcz przeciwnie? Będziemy dążyć do ułatwień i odejdziemy od podawania haseł do kont czy wieloskładnikowego uwierzytelniania? A może wiele metod weryfikacji naszej tożsamości zastąpi biometria?

– Moim zdaniem Internet będzie coraz szerzej wykorzystywany i to będzie wymuszało coraz większą ochronę prywatności, coraz więcej metod weryfikacji zastąpi biometria i pewnie pojawią się nowe formy zabezpieczeń, których w tej chwili jeszcze nie znamy.