Cyfrową maseczkę noś cały czas

Czy pamiętacie, jak noszono maseczki w czasie pierwszych fal pandemii COVID-19? Maseczki, które miały uchronić przed zakażeniem. Nawet w najtragiczniejszym okresie, gdy wiele osób umierało, a szpitale ledwo wyrabiały się z przyjmowaniem pacjentów, maseczki noszono na brodzie, pod nosem, w kieszeni lub na łokciu. I nie pomagały apele lekarzy, by szczelnie zasłaniać usta i nos. Skoro ludzie nie przestrzegali zasad higieny przy bezpośrednim zagrożeniu zdrowia i życia, to czy będą przestrzegać zasad cyberhigieny?

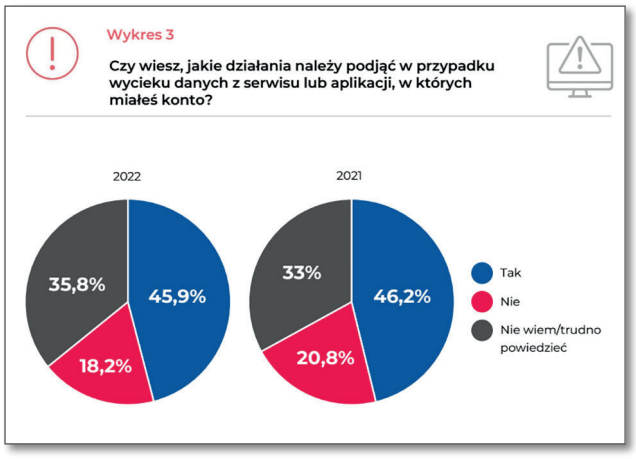
Joanna Karczewska
One of Europe's Top Cyber Women

Żeby skutecznie chronić się w cyberprzestrzeni, należy wiedzieć przed czym i jak. W marcu 2022 r. ukazał się raport z badania „Poziom wiedzy finansowej Polaków 2022", opublikowany przez Warszawski Instytut Bankowości i Fundację GPW w przededniu VI Kongresu Edukacji Finansowej i Przedsiębiorczości. Okazuje się, że najważniejszym tematem „pierwszej potrzeby" jest cyberbezpieczeństwo, bowiem ponad połowa Polaków odczuwa brak wiedzy w tym obszarze. Istotnie częściej wskazują go osoby w wieku 25–34 lata.

Brak wiedzy potwierdza badanie przeprowadzone w styczniu 2022 r. przez Santander Consumer Bank na rzecz kolejnego raportu z serii „Polaków Portfel Własny" (https://www.blog.santanderconsumer.pl/blisko-ciebie/wiekszosc-polakow-nie-zna-podstawowych-pojec-dotyczacych-cyberbezpieczenstwa,1,153.html). Okazało się, że większość Polaków ma duży problem z pojęciami dotyczącymi cyberbezpieczeństwa. Ponad 60 proc. ankietowanych nie potrafiło powiedzieć, co to jest chargeback, phishing czy skimming. Tylko co czwarty ankietowany stwierdził, że jego zasób wiadomości na temat niebezpieczeństw związanych z korzystaniem z internetu jest na zdecydowanie dobrym poziomie (24 proc.), w tym najwięcej 18–29 latków (42 proc.). Co trzeci ocenił go na 3 (33 proc.), a co dziesiąty na 2 (ok. 11 proc.) w skali od 1 do 5, gdzie ocena 5 oznaczała najwyższy poziom wiedzy, a 1 najniższy.

Zatem nie dziwi, że „**ponad połowa Polaków nie wie, jak zareagować w przypadku wycieku danych osobowych**", co radośnie obwieścił Urząd Ochrony Danych Osobowych, podsumowując badanie przeprowadzone także w marcu 2022 r. na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu (https://uodo.gov.pl/pl/138/2404).

Raport z badania składa się z dwóch części: „Wiedza na temat bezpieczeństwa danych osobowych w Polsce" oraz „Cyberzagrożenia – czego boją się Polacy?".



Zastanawia i niepokoi spadek liczby osób, które sądzą, że wiedzą. Zastanawia także brak orientacji wśród respondentów, jak poradzić sobie z konsekwencjami wycieków. Zdaniem 70 proc. ankietowanych jest to zadanie policji i innych służb ścigania, np. prokuratury. 60 proc. wskazuje na firmę lub instytucję będącą administratorem bazy danych, z której te wyciekły, ponad 56 proc. wskazuje na UODO, 44 proc. – na inspektorów ochrony danych z instytucji i firm, z których te wyciekły, a co trzeci ankietowany uważa, że neutralizacją skutków powinna zająć się osoba, której dane wyciekły.

Co jeszcze stwierdzono? Chociażby to, że pomimo przekonania o swojej wiedzy i wysokim poczuciu własnego bezpieczeństwa młodzi Polacy są grupą, która najczęściej popełnia błędy w postaci publikacji zdjęć swoich dokumentów w sieci, udostępniania osobom trzecim loginów i haseł do logowania oraz zostawiania danych osobowych w internetowych ankietach.

Wiemy, ale nie powiemy

W lipcu 2022 r. Prezes UODO nałożył karę administracyjną na Uniwersyteckie Centrum Kliniczne Warszawskiego Uniwersytetu Medycznego (https://uodo.gov.pl/pl/138/2428) za:

- niezgłoszenie Prezesowi UODO naruszenia ochrony danych osobowych oraz
- niezawiadomienie o naruszeniu osoby, której dane dotyczą.

Naruszenie polegało na ujawnieniu, w wyniku błędu lekarza wystawiającego skierowanie do poradni specjalistycznej, danych osobowych osobie nieuprawnionej (innemu pacjentowi administratora) w zakresie: nazwisko, adres zamieszkania, numer ewidencyjny PESEL oraz informacje o stanie zdrowia.

Zszokowało mnie kalendarium zdarzeń:

2021 – marzec	Prezes UODO otrzymał informację od Rzecznika Praw Pacjenta o możliwości zaistnienia naruszenia ochrony danych osobowych.
2021 – kwiecień	Prezes UODO zwrócił się do administratora o udzielenie informacji.
2021 – kwiecień	Odpowiedź administratora.
2021 – lipiec	Prezes UODO wszczął z urzędu postępowanie administracyjne.
2021 – sierpień	Odpowiedź administratora.
2022 – 6 lipca	Decyzja Prezesa UODO.

Od zgłoszenia naruszenia do UODO do wydania decyzji minęło 15 miesięcy. W tym czasie osoba poszkodowana żyła w błogiej nieświadomości, że jej dane otrzymała inna osoba. Administrator nie uznał za stosowne ją zawiadomić „ze względu na okoliczność, iż incydent nie wywiera znaczących skutków dla praw i obowiązków osoby, której dane dotyczą". Takiego rozumowania nie uznał prezes UODO i wytłumaczył w uzasadnieniu decyzji, że:

- „Zawiadamiając bez zbędnej zwłoki podmiot danych, administrator umożliwia osobie podjęcie niezbędnych działań zapobiegawczych w celu ochrony praw lub wolności przed negatywnymi skutkami naruszenia."

- „Administrator podejmując zatem decyzję o niezawiadomieniu o naruszeniu organu nadzorczego, jak i osób, których dane dotyczą, w praktyce pozbawił te osoby, przekazanej bez zbędnej zwłoki, rzetelnej informacji o naruszeniu i możliwości przeciwdziałania potencjalnym szkodom."

- „Za okoliczność obciążającą Prezes UODO uznaje długi czas trwania naruszenia. Od powzięcia przez administratora informacji o naruszeniu ochrony danych osobowych do dnia wydania niniejszej decyzji upłynęło kilkanaście miesięcy, w trakcie których ryzyko naruszenia praw lub wolności osoby dotkniętej naruszeniem mogło się zrealizować, a czemu osoba ta nie mogłaby przeciwdziałać ze względu na niewywiązanie się przez administratora z obowiązku powiadomienia jej o naruszeniu".

Skoro brak zawiadomienia był i jest tak istotny, to dlaczego urząd sam nie powiadomił osoby poszkodowanej o incydencie? Bo nie ma ustawowego obowiązku? Prawie rok trzymał pisma w szufladzie, zanim wydał decyzję, by mieć pretensje do administratora? Nie rozumiem postępowania urzędu.

Wiemy i wykorzystamy

Nie tylko w tym przypadku osoba zainteresowana nie wiedziała o naruszeniu ochrony jej danych osobowych. Jak poinformował CERT Polska w swoim raporcie z działalności, w 2021 r. zarejestrował łącznie 29 483 unikalne incydenty cyberbezpieczeństwa i odnotował wzrost obsłużonych incydentów o 182 proc. w porównaniu do roku 2020. Najczęstszym typem był phishing – stanowiący aż 76,57 proc. wszystkich obsłużonych incydentów. Jest to wzrost o 196 proc. w porównaniu do poprzedniego roku. Zaznaczył, że „wykradzione informacje mogą zostać odsprzedane lub wykorzystane jako punkt wyjścia do popełniania kolejnych oszustw. Tego typu dane są więc popularnym towarem na czarnym rynku i są chętnie wykradane". A my często nie wiemy o kradzieży.

Sama w dość zaskakujący sposób przekonałam się o nieustającym wykorzystywaniu naszych danych bez naszej wiedzy. Otóż 8 lipca 2022 r. dostałam e-mail wysłany przez Wyższą Szkołę Bankową w Warszawie z reklamą m.in. studiów podyplomowych z ochrony danych osobowych oraz

zarządzania cyberbezpieczeństwem. Nadawca twierdził, że ma moje zgody na:

- otrzymywanie od administratora danych osobowych informacji handlowej i materiałów promocyjnych środkami komunikacji elektronicznej w rozumieniu ustawy o świadczeniu usług drogą elektroniczną;

- kontakt ze strony administratora danych osobowych, z użyciem telekomunikacyjnych urządzeń końcowych oraz automatycznych systemów wywołujących, zgodnie z art. 172 par. 1. Prawa telekomunikacyjnego;

- przetwarzanie moich danych osobowych przez administratora danych osobowych w celach marketingowych i reklamowych.

Dane są także udostępnianie przez nas samych. Raport organizacji Irish Council for Civil Liberties z maja 2022 r. o skali zautomatyzowanego zakupu powierzchni reklamowej w czasie rzeczywistym w modelu aukcyjnym w USA i Europie (ang. „ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe"), słusznie zatytułowany „The Biggest Data Breach" (https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/), pokazuje zatrważającą skalę codziennego handlu naszymi danymi przez operatorów różnych portali i aplikacji. Są to dane – także z Polski – o naszym zachowaniu w internecie, nierzadko bardzo wrażliwe.

Otóż nie miał i nie ma. Po kliknięciu w podane linki, okazało się, że za wysyłką stoi firma marketingowa dostarczająca „wysokiej jakości platformę Marketing Automation". Bez zbędnej zwłoki, czyli na drugi dzień, o wyjaśnienie sytuacji zwróciłam się do Inspektora ochrony danych, a następnie do Prorektora WSB w Warszawie. Nadal czekam na odpowiedź.

Wiemy i powiemy

Wiele podmiotów ma za zadanie „prowadzenie działań z zakresu budowania świadomości w obszarze cyberbezpieczeństwa" bądź poczuwa się do realizacji takiego zadania. W związku z tym jest mnóstwo inicjatyw różnych ministerstw, urzędów, banków, firm, organizacji pozarządowych i innych podmiotów. Właściwie trwa konkurs „piękności", kto wyda ładniejsze publikacje i zorganizuje lepsze szkolenie czy webinarium. Trwa też wyścig o fundusze unijne. Dla przykładu, Program wieloletni na rzecz Osób Starszych „Aktywni+" realizowany przez Departament Polityki Senioralnej Ministerstwa Rodziny i Polityki Społecznej zawiera priorytet nr 3, czyli włączenie cyfrowe, które obejmuje pomoc osobom starszym wykluczonym cyfrowo, polegającą na zwiększeniu ich umiejętności w posługiwaniu się nowoczesnymi technologiami oraz zapewnieniu bezpiecznego funkcjonowania przy wykorzystywaniu współczesnych narzędzi cyfrowych (http://senior.gov.pl/aktualnosci/pokaz/602). Żadnego z oferentów, którzy wygrali otwarty konkurs ofert dla priorytetu nr 3 edycji 2022, nie kojarzę jako organizacji zajmującej się na co dzień wzmacnianiem świadomości w obszarze zagrożeń pochodzących z cyberprzestrzeni oraz budowaniem systemu cyberbezpieczeństwa czy ochrony danych osobowych w Polsce. Ciekawe, skąd biorą materiały do szkoleń i jak je prowadzą.

Czy i gdzie Polacy szukają informacji i zaleceń dotyczących cyberbezpieczeństwa?

Badanie Santander Consumer Bank

Większość Polaków (80 proc.) przyznała, że przynajmniej raz w życiu próbowała na własną rękę dowiedzieć się więcej na temat cyberbezpieczeństwa. Może to zwiastować, że z czasem nasza wiedza poprawi się, zwłaszcza jeżeli będziemy korzystać z godnych zaufania źródeł, np. strony internetowej banku lub urzędu. Według naszego badania, co najmniej raz z tego sposobu zdobywania wiedzy korzystało 56 proc. Polaków. Popularnymi źródłami były również artykuły online (63 proc.), znajomi (33 proc.) i media społecznościowe (40 proc.).

Badanie ChronPESEL.pl i Krajowego Rejestru Długów

O bezpieczeństwie danych osobowych najchętniej rozmawiamy ze znajomymi (blisko 2/3 ankietowanych).

Nie zadano ankietowanym pytania, skąd czerpią wiedzę o zasadach zapewnienia bezpieczeństwa danych osobowych.

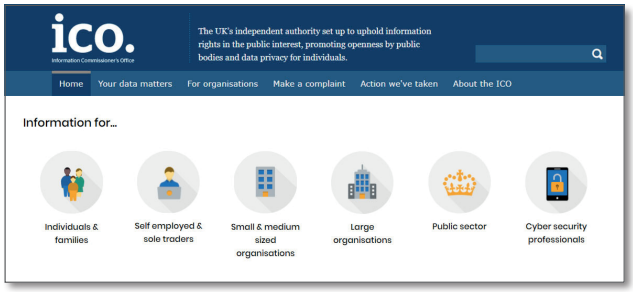
Raport CERT Polska za 2021

CERT Polska: zachęcamy do przeczytania materiału o tworzeniu i używaniu haseł w bezpieczny sposób, który znaleźć można na naszej stronie internetowej. Zachęcamy do śledzenia naszych mediów społecznościowych na portalu Facebook (https://fb.com/CERT.Polska) oraz na Twitterze (@CERT_Polska), gdzie informujemy o obserwowanych przez nas bieżących scenariuszach oszustw i innych zagrożeniach wymierzonych w polskich internautów.

> *Krótko mówiąc, Polacy nie wiedzą, gdzie szukać wiedzy.*

Jakże zazdroszczę Brytyjczykom. U nich są dwa podstawowe źródła informacji:

- National Cyber Security Centre (NCSC) z genialną stroną www.ncsc.gov.uk



- Information Commissioner's Office – odpowiednik naszego UODO – z mega przyjazną stroną ico.org.uk

Na obu stronach zalecenia są udostępniane według aktualności, adresatów czy tematów – wystarczy przewinąć lub wyszukać. Oba podmioty ściśle ze sobą współpracują, zaś ich rekomendacje są spójne i skorelowane. Owszem, są też inne inicjatywy, ale każdy w Wielkiej Brytanii kojarzy obie instytucje jako wiodące i najbardziej wiarygodne w kwestiach cyberbezpieczeństwa i ochrony danych osobowych. Sama dużo korzystam z ich materiałów i webinariów.

Wiemy i nie powiemy

Strategia Cyberbezpieczeństwa RP na lata 2019–2024 zawiera Cel szczegółowy 4 – Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa, który obejmuje m.in.:

- stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli,

- rozwijanie świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni.

W dniu 6 lipca 2022 r. Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu RP rozpatrywała informację ministra cyfryzacji na temat realizacji Strategii Cyberbezpieczeństwa na lata 2019–2024. Liczyłam na przedstawienie konkretnych działań podjętych w ramach realizacji celu 4 i rozwinięcie odpowiedzi przesłanej do ENISA. Okazało się, że tylko posłowie – członkowie Komisji otrzymali obszerną pisemną informację, zaś minister Janusz Cieszyński w swoim wystąpieniu skupił się na najważniejszych elementach, które nie obejmowały celu 4. Korzystając z obecności na posiedzeniu Komisji, poprosiłam m.in. o komentarz do wyników badań WIB oraz KRD (wymienione na początku artykułu). Zamiast odpowiedzi otrzymałam propozycję spotkania. Nadal czekam na zaproszenie.

Co trzeba wiedzieć

W trakcie pandemii byliśmy zasypywani informacjami o sposobach ochrony: szczepienia, pomiary temperatury, dystans społeczny, maseczki, kwarantanny itd. W kwestii cyberhigieny przeciętny Kowalski i przeciętna Kowalska są zdani na siebie.

W publikacji ENISA „Raising awareness of cybersecurity – A Key Element of National Cybersecurity Strategies" wydanej w listopadzie 2021 r., na pytanie: ***Greatest challenge(s) relative to cybersecurity awareness***

strona polska odpowiedziała: ***The problem appears to be in moving from awareness to execution; practicality and implementation are always challenges.***

Minęło 6 lat wrzawy wokół RODO i 4 lata budowy krajowego systemu cyberbezpieczeństwa, a w Polsce nadal nie opracowano i nie wdrożono czytelnego i spójnego systemu informowania użytkowników cyberprzestrzeni o zagrożeniach i sposobach przeciwdziałania. Różne instytucje państwowe i podmioty prywatne „na wyścigi" podejmują różne działania edukacyjne, powodując szum informacyjny. Każdy kolejny raport dotyczący stanu cyberbezpieczeństwa czy ochrony danych osobowych pokazuje całą mizerię organizowanych akcji i kampanii. A przecież każda Polka i każdy Polak powinni wiedzieć, że

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 21 sierpnia 2022 r.