Bezpieczne korzystanie z narzędzi e-administracji

W Polsce cyfryzacja państwa i urzędów to proces, który rozpoczął się wiele lat temu. Powstają kolejne e-bazy, ułatwiające funkcjonowanie administracji, zwiększające dostępność danych, a także poziom ich ochrony. Paleta e-rozwiązań państwowych jest bardzo duża, ale czy potrafimy z nich korzystać bezpiecznie?
Z chwilą kiedy zaczęły powstawać udogodnienia ważne dla obywateli to nastąpiło ich znaczące przyspieszenie. Wystarczy przypomnieć, że liczba użytkowników Profilu Zaufanego między 2016 a 2023 rokiem zwiększyła się z około 400 tysięcy do ponad 16 milionów. Jest to jednak jedno z wielu dostępnych rozwiązań w wirtualnej przestrzeni ułatwiających kontakt obywatelowi z administracją.

Obecnie obywatele mogą skorzystać z kilkuset e-usług publicznych zlokalizowanych na różnych platformach i portalach rządowych. Wśród nich są: Elektroniczna Platforma Usług Administracji Publicznej (ePUAP), Platforma Usług Elektronicznych Zakładu Ubezpieczeń Społecznych (PUE ZUS), portal obywatel.gov.pl, portal biznes.gov.pl.

E-podatki, e-recepta, i mObywatel
Jest wiele platform i technologii, które wspierają nas w różnych aspektach życia codziennego. Do jednych z najbardziej znanych i popularnych jest na przykład Portal Pacjenta. Na platformie możemy znaleźć bez trudu informacje dotyczące e-recepty, skierowania do specjalistów, historię leczenia, a także zwolnienia lekarskie. Dodatkowo po podaniu takich informacji jak numer telefonu lub adres e-mail, będziemy mogli otrzymać w formie SMS-a recepty, lub wysłane na naszą skrzynkę mailową. Na podobnej zasadzie na innych platformach, możemy rozliczyć PIT czy napisać odpowiedni dokument do urzędu.
Aplikacja mObywatel dostępna jest od 2017 roku, która cały czas jest rozwijana i uzupełniana o nowe funkcjonalności. To właśnie w tej aplikacji możemy m.in. skorzystać z mDowodu czyli nowego elektronicznego dokumentu tożsamości ważnego w Polsce, a także z elektronicznego odpowiednika naszego prawa jazdy, legitymacji emeryta/rencisty czy legitymacji szkolnej, a nawet z Karty Dużej Rodziny. Dodatkowo możemy znaleźć tam wiele dodatkowych usług od możliwości zgłoszenia naruszeń środowiskowych, czy nawet opcję sprawdzenia punktów karnych.

Ochrona danych w świecie e-usług publicznych
Państwo przykłada dużą wagę do zapewnienia cyberbezpieczeństwa naszych danych. Możemy tak wnioskować choćby z przyjętej niedawno ustawy, dzięki której do 2026 r. ma powstać Krajowe Centrum Przetwarzania Danych. Wartość inwestycji to ponad 1 mld zł. Będzie więc możliwy dalszy rozwój e-usług rządowych z zapewnieniem koniecznego poziomu ochrony danych.
Jednak nawet najlepsze zabezpieczenie nie wystarczy. **Nasz poziom ochrony w sieci zależy również od naszej wiedzy jak i przede wszystkim czujności.** Z tego powodu dobrze uwzględnić kilka dodatkowych praktycznych wskazówek.

Elektroniczna Platforma Usług Administracji Publicznej (ePUAP)
Warunkiem korzystania z elektronicznej platformy usług administracji publicznej (ePUAP) oraz konta mObywatel będzie wymagało od nas podania imienia (imion) i nazwiska, numeru PESEL, adresu e-mail, numeru telefonu komórkowego oraz określenia niepowtarzalnego identyfikatora użytkownika.
To oznacza, że w celu identyfikacji i uwierzytelnienia użytkownik może zastosować określone przez siebie: **identyfikator użytkownika i hasło** albo np. kwalifikowany certyfikat. W przypadku zastosowania hasła stopień jego złożoności kontrolowany jest przez ePUAP. To pozwala na wstępne ustalenie czy nasze hasło jest „bezpieczne".

Ustawienie hasła
Korzystanie z e-administracji podobnie jak z innych internetowych usług będzie wymagało ustawienia „silnego" hasła. Według najnowszych badań mniej niż połowa (48%) użytkowników internetu stosuje odpowiednio silne hasła. Jeżeli chcemy, aby było ono bezpieczne, **to powinno być odpowiednio długie i zawierać cyfry i znaki specjalne**. Pomocne mogą okazać się gotowe generatory oraz tzw. menedżerowie haseł.
Uwaga na maile czy telefony z urzędu
Korzystając z e-administracji podajemy najczęściej dwie formy kontaktu czyli numer telefonu i adres poczty elektronicznej. Zdarza się, że instytucje wysyłają jakąś wiadomość mailową. **Jeśli jej treść nas zaniepokoiła to co powinniśmy zrobić?**

W pierwszej kolejności należy przeanalizować jej treść w poszukiwaniu **nieprawidłowości takich jak literówka w adresie**. Również sama treść może zawierać jakieś dziwne błędy, urwane zdanie itd. Jeśli masz jakiekolwiek wątpliwości, to najlepiej skontaktuj się bezpośrednio z daną jednostką inną drogą, np. za pomocą oficjalnej infolinii.
Nie korzystaj jednak z numeru telefonu podanego w treści maila, lecz poszukaj go na oficjalnej stronie danego urzędu. Poza tym, przede wszystkim **unikaj klikania w niezweryfikowane linki** i podawania informacji o sobie, dopóki nie upewnisz się, że to bezpieczny kontakt.

Aktualizacja aplikacji
Jeżeli korzystamy z aplikacji na telefonie to należy pamiętać, że to narzędzie również wymaga stałego unowocześniania zabezpieczeń. Najczęściej aplikacja z której korzystamy sama wyświetli nam komunikat o pojawianiu się najnowszej aktualizacji. To najlepsza metoda, aby uniknąć luk w ochronie naszej aplikacji, które mogą wykorzystać cyberprzestępców. Dlatego **nie powinniśmy odkładać w czasie przeprowadzenia aktualizacji** naszej aplikacji, bo im dłużej będziemy zwlekać tym rośnie niebezpieczeństwo, że ktoś wykradnie nasze dane.

Ściągaj aplikacje tylko z zaufanego źródła
Jeżeli chcemy skorzystać z danej aplikacji to wybieramy **najbardziej wiarygodne źródło**. Jedynie w ten sposób uzyskamy gwarancję, że jest to bezpieczne narzędzie, a nie aplikacja-pułapka. Jeżeli już ściągnęliśmy daną aplikację, a nie mamy pewności czy pochodzi ono z wiarygodnego źródła to bez jej otwierania starajmy się ją usunąć z telefonu. Jeżeli mamy na smartfonie zamontowany program antywirusowy to dla bezpieczeństwa powinniśmy go uruchomić. Dopiero po tej operacji próbujemy na nową ściągnąć aplikację, ale już z wiarygodnego źródła.

Artykuł przygotowany w ramach kampanii edukacyjnej realizowanej przez Fundację Warszawski Instytut Bankowości pod patronatem Ministerstwa Cyfryzacji pn. „@ktywnie w sieci", trwającej w terminie 10.10.-10.12.2024 r.