Ludzie nie zawsze potrafią zidentyfikować ryzyko, a wielu ma problem z rozpoznaniem fałszywych wiadomości, poprzez które oszuści próbują wyłudzić dane osobowe.

Nieustannie warto przypominać, że najważniejsza jest zasada ograniczonego zaufania i zachowywanie zdrowego rozsądku. Tylko ostrożność oraz dokładne weryfikowanie informacji i internetowych kontaktów pozwoli ograniczyć ryzyko zdobycia przez przestępców dostępu do naszych danych osobowych.

1. Uważaj na to, co i komu udostępnisz o sobie

Nie udostępniaj pochopnie danych osobowych nieznanym osobom i podmiotom. Nie bój się pytać, kim są, co uprawnia ich do pozyskiwania Twoich danych, po co je zbierają.

Rozmyślnie dysponuj swoimi danymi, w szczególności w mediach społecznościowych, które mogą być kopalnią wiedzy o Tobie czy Twojej rodzinie. Dla przykładu unikaj publikowania zdjęć dokumentów.

2. Nie zostawiaj dokumentów w zastaw

Nie oddawaj w zastaw dowodu osobistego, paszportu, prawa jazdy. Zgodnie z prawem zatrzymywanie dowodu osobistego bez podstawy prawnej jest karane, natomiast nie wszystkie dane osobowe zawarte we wskazanych dokumentach są niezbędne dla realizacji celu.

Co do zasady nie powinieneś się godzić na kopiowanie dokumentu tożsamości. Tylko w niektórych sytuacjach jest to wyjątkowo dopuszczalne, gdy pozwalają na to przepisy. Gdy administrator domaga się kopii np. dowodu osobistego, poproś, aby wskazał Ci podstawę prawną, która nakłada na niego obowiązek takiego działania.

3. Nie podawaj danych przez telefon, gdy nie jesteś pewien, że to konieczne

Unikaj przekazywania danych telefonicznie – szczególnie, gdy to nie Ty inicjujesz rozmowę, ale ktoś dzwoni do Ciebie. Udostępnianie danych na odległość obarczone jest ryzykiem, brakiem pewności co do tego komu faktycznie dane są przekazane. Nie daj się zaskoczyć, sprowokować do udostępniania danych wbrew Twojej woli, dla nieznanych, niewyjaśnionych przez rozmówcę celów. Upewnij się, komu faktycznie udostępniasz dane w trakcie rozmowy telefonicznej, a jeżeli trzeba zweryfikuj kontakt, np. oddzwaniając i sprawdzając, czy dany numer i osoba faktycznie reprezentuje podmiot, na który się powołała.

4. Uważaj na różne formularze, poprzez które udostępniasz dane

Zachowaj rozwagę przy wypełnianiu i podpisywaniu różnego rodzaju ankiet, formularzy czy umów. Zastanów się, czy faktycznie chcesz założyć kartę lojalnościową w sklepie, by mieć rabaty lub dodatkowe promocje. Czy rzeczywiście warto oddać swoje dane osobowe w zamian za promocje, bony rabatowe, dodatkowe upominki do zakupów? W takich sytuacjach podajesz zbiór danych jak imię, nazwisko, adres zamieszkania, datę urodzenia, numer telefonu, a w zamian otrzymujesz promocje, bony rabatowe, dodatkowe upominki przy zakupach.

5. Nie podawaj wszelkich danych

Nie podawaj danych nadmiarowych, które pozwalają na pełną identyfikację, jeżeli w danej sytuacji nie jest to konieczne. Jeśli musisz skorzystać z danej usługi, to podaj tylko dane niezbędne do jej wykonania – dobrze przemyśl przekazanie tych informacji, które możesz podać opcjonalnie.

6. Nie wyrażaj zgody pochopnie

Wypełniając formularz, zanim zaznaczysz wszystkie zgody, upewnij się, czego dotyczą. Zwróć uwagę, czy w formularzu zgody nie są zaznaczone domyślnie. Zgodnie z prawem nie powinno tak być. Dokładnie też czytaj, czego dotyczą klauzule zgód. W przypadku wątpliwości, zadawaj pytania administratorom. Powinni Cię poinformować o okresie przez jaki dane będą przetwarzane oraz o przysługujących Ci prawach, w tym dostępu do danych, ich sprostowania, usunięcia czy wniesienia sprzeciwu wobec przetwarzania, a także, czy Twoje dane będą komuś innemu (innym odbiorcom) przekazywane.

Pamiętaj, że wyrabiając kartę lojalnościową, często udzielasz zgód na wykorzystywanie danych w celach marketingowych nie tylko administratora, ale i jego partnerów biznesowych. O ile możesz, zweryfikuj, kim oni są, jakie to są firmy i ile ich jest, gdyż krąg podmiotów, którym udostępnione są dalej dane potrafi być bardzo szeroki. Zgody na tzw. „cudzy" marketing nie mogą być obowiązkowe – powinna być Ci pozostawiona możliwość wyboru co do tego, czy taką zgodę wyrazisz.

7. Nie wyrzucaj danych na śmietnik, dopóki ich nie zniszczysz

Wszelkie dokumenty z Twoimi danymi, to kolejne źródło wiedzy o Tobie, zwłaszcza gdy zawierają one wiele różnych informacji umożliwiających wyciągania wniosków na Twój temat. Dlatego też – zanim wyrzucisz dokumenty do kosza – należy je zniszczyć (np. faktury, rachunki zapiski, naklejki na opakowaniach od korespondencji czy po dostarczonych towarach) w sposób uniemożliwiający odtworzenie zawartych w nich danych osobowych.

8. Bądź czujny, czytając korespondencję

Każda osoba powinna bardzo dokładnie czytać otrzymywaną korespondencję. Przestępcy potrafią przygotować wiadomości do złudzenia przypominające te, które dostajemy z banków, firm kurierskich czy platform sprzedażowych. Mogą też dysponować pewnym zestawem danych na nasz temat i przygotować spersonalizowaną wiadomość pod kątem usług, z jakich korzystamy na co dzień.

9. Zwracaj uwagę, kto jest nadawcą maila

Nie odpowiadaj na maile od osób, których nie znasz np. od tzw. spamerów, zwłaszcza gdy domagają się podania jakichś informacji o Tobie czy namawiają do kliknięcia w przesłany link lub otwarcia przesłanego załącznika, sugerują zmianę identyfikatora i hasła.

10. Sprawdź strony internetowe, z których korzystasz

Zachowaj ostrożność także przy korzystaniu z usług bankowości elektronicznej i dokonywaniu zakupów przez Internet. Zwracaj uwagę, czy aby na pewno logujesz się do serwisu bankowości internetowej ze strony banku, która ma certyfikat SSL (widoczny w pasku adresu przeglądarki).

11. Sprawdź, czy dany podmiot w ogóle istnieje

Weryfikuj sklepy, w których chcesz coś kupić: czy w ogóle istnieją, czy i jakie mają opinie, czy są to podmioty zidentyfikowane, gdzie mają siedzibę, czy podany jest kontakt z ich właścicielem i czy kontakt ten nie jest ograniczony tylko do elektronicznego.

12. Weryfikuj regulaminy i polityki prywatności

Unikaj sprzedawców nieprzedstawiających takich dokumentów czy też prezentujących w nich postanowienia zbyt ogólne, niejasno, lub nieprecyzyjnie brzmiące, sformułowane niepoprawnie gramatycznie czy językowo. Może to bowiem oznaczać, że są to podmioty niepodlegające polskiemu czy europejskiemu prawu.

13. Używaj programów chroniących komputer

Korzystasz z komputera? Tableta? Smartphona? Używaj oprogramowania chroniącego komputer i urządzenia mobilne przed niepożądanymi działaniami z zewnątrz, np. złośliwego oprogramowania. Oprócz popularnych programów antywirusowych przydatne mogą być również te, które zabezpieczą przed ingerencją z zewnątrz tzw. firewall.

14. Zadbaj o silne hasła

Dla własnego bezpieczeństwa warto stosować różne hasła do różnych systemów i nie udostępniać ich innym osobom. Dobrze jest, aby nie miały one nic wspólnego z Twoimi życiem osobistym, miejscem zamieszkania, Twoim imieniem i nazwiskiem, datą urodzin, imionami Twoich bliskich czy Twoich zwierząt itp.

Nie powinno się też zapisywać ich na kartce papieru czy w notesie. Najlepiej jest je zapamiętywać, co jest dużą sztuką, gdy musimy logować się do wielu serwisów. Pomocne w tym zakresie mogą być np. darmowe menadżery haseł, które umożliwiają nie tylko generowanie odpowiednio trudnych do złamania haseł, ale i zapamiętują je za nas. Tym samym łatwiejsza jest częstsza zmiana haseł, a ryzyko, że ktoś je pozna maleje.

Utrata kontroli nad danymi osobowymi może narazić Cię na posłużenie się nimi bez Twojej wiedzy i woli, co z kolei stwarza niebezpieczeństwo kradzieży tożsamości. Osoby dysponujące kompletem informacji o Tobie mogą podszyć się pod Ciebie i np. dokonywać na Twoją szkodę różnych transakcji, takich jak chociażby zaciągnięcie kredytu w banku czy wypożyczenie drogiego sprzętu i niezwrócenie go .

Inspektor Ochrony Danych w ZUT- mgr Artur Kurek